Release by TEAM-DZ

NOUVEAU

Le Guide Référence

130 PAGES D'EXPERTISE

N°4

SÉCURISEZ VOTRE PC !

DÉPANNEZ | SAUVEGARDEZ | DÉFENDEZ

L'ESSENTIEL POUR NAVIGUER SANS RISQUE

Et aussi ...

- Accédez plus vite à Internet
- Sécurisez Facebook
- Désinfectez votre PC
- Échappez aux crash disque

PLUS DE 200 ASTUCES POUR AMÉLIORER VOTRE PC

Release by TEAM-DZ

EN VENTE ACTUELLEMENT

GRATUIT : 2 CD-ROM

windowsnews.fr

Windows news

L'expert conseil de votre micro

N° 204
Juin 2011

Logiciel complet !
Dopez votre PC avec TuneUp Utilities

Exclusif Le premier test de Windows 8 en avant-première !

Les nouvelles versions changent tout

NAVIGATEURS WEB

CHOISISSEZ LE MEILLEUR !

LE VERDICT DE LA RÉDACTION

- ✔ Le plus rapide
- ✔ Le plus sûr
- ✔ Le plus ouvert

COMPARATIF
5 SSD de 256 Go

COMPARATIF
12 logiciels pour

NOUVEAU !

CAHIER EXPERT
Serveur | Cloud | Administration

COMMENT S'ÉQUIPER D'UN NAS ?

le guide pour s'équiper d'un NAS

+

2 CD-ROM

TUNE UP UTILITIES™ 2011 !

(logiciel complet valable 90 jours)

TuneUp Utilities 2011
PRODUIT COMPLET
Windows

Windows news
LOGICIELS
CD 2 CD-ROM GRATUIT JUIN 2011

28 SOFTS pour doper votre navigation

- Boostez la vitesse de téléchargement
- Bloquez les bannières publicitaires
- Capturez à la volée les images et vidéos

Plus de 40 logiciels pour...
MIEUX GÉRER SON PC
LE TRAVAIL DISTANT

Release by TEAM-DZ

Windows news Guide Référence n°4 est édité par Yellow Media S.A.S. au capital de 1 218 475 euros.
Immatriculée au RCS de Nanterre B 388 330 417

Siège social
101-109, rue Jean-Jaurès 92300 Levallois-Perret
Tél. : 01 41 27 38 38 – Fax : 01 41 27 38 39
www.mesmagazinesfavoris.fr
Présidente directrice générale : Saghi Zaïmi
Directrice générale finance et administration : Jane Méline
Principal actionnaire : WM7
Directrice de la publication : Saghi Zaïmi
Directrice des ressources humaines : Marguerite Gautier (jobs@yellowmedia.fr)
Directrice marketing et commercial : Saghi Zaïmi
Directeur de magazine : Vincent Alexandre
Prix au numéro : 8,50 €

Rédaction
Directeur éditorial : Joscelyn Flores
Rédacteur en chef : Thierry Outrebon
Chefs de rubriques : Bruno Mathieu, Arnaud Dimberton
Première secrétaire de rédaction : Isabelle Compoint
Première rédactrice graphiste : Jennyfer Buzenac
Assistant de rédaction : Cédric Dessillons
Chef de studio : Frédéric Thibault
Ont collaboré à ce numéro : Sandrine Beauvais, Jean-Pierre Carles, Anne Daubrée, Jean-Marc Delprato, Jean-François Demay, Loïc Duval, Ahmed Kheloufi, Pierre-Édouard Laurent, Jean-Paul Mesters, Ratana Mey, Benoît Moyen, Marc Olanié, Thierry Pigot.

Publicité
Tél. : 01 41 27 38 38 – Fax : 01 41 27 38 00
Directeur exécutif : Jérôme Adam (jerome.adam@yellowmedia.fr)
Directeurs de la publicité : Myriam Maman (myriam.maman@yellowmedia.fr), Médéric Breton (mederic.breton@yellowmedia.fr), Cyril Monod (cyril.monod@yellowmedia.fr), François Lamrani (françois.lamrani@yellowmedia.fr)
Chef de publicité : Alexandre Meunier
Responsable trafic : Maguy Édouard (maguy.edouard@yellowmedia.fr)
Assistante trafic : Nathalie Lopes

Fabrication
Responsable de la fabrication : Philippe Perrot (philippe.perrot@yellowmedia.fr)
Chargée de fabrication : Jessica Walter (jessica.walter@yellowmedia.fr)

Diffusion
Directeur de la diffusion : Vincent Alexandre
Chef de produit vente au numéro : Jacky Cabrera
Vente d'anciens numéros : 01 44 84 05 50
Diffusion : MLP
Impression : Stige S.p.A
siège social : San Mauro Torinese (TO)
Imprimé en Italie, printed in Italy
Dépôt légal : à parution
Commission paritaire : 1113 K 84436
ISSN : 2112-4345
Copyright Yellow Media - © 2011. Tous droits de reproductions réservés.
Windows news est une marque déposée.
La rédaction n'est pas responsable des textes, illustrations et photos qui lui sont communiqués par leurs auteurs. La reproduction totale ou partielle des articles publiés dans Windows news Le Guide Référence est interdite sans accord écrit de la société Yellow Media. Sauf accord particulier, les manuscrits, photos et dessins adressés à Windows news Le Guide Référence, publiés ou non, ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire. Ce numéro contient pour la totalité des exemplaires un CD-ROM promotionnel, qui ne peut être vendu séparément.

Microsoft, Windows, Windows 95, Windows 98, Windows XP, Vista et Windows 7 sont des marques déposées par Microsoft Corporation. Windows® est une marque déposée de Microsoft Corporation.

LÉGITIME DÉFENSE NUMÉRIQUE

Le piratage est devenu le fléau informatique N°1 et l'essentiel des activités de maintenance des PC tient de plus en plus à la mise à jour des bases d'antivirus et de vérification des fichiers potentiellement ciblés. Le PC tombe de moins en moins en panne pour des raisons électroniques mais se trouve victime de plus en plus de blocages logiciels liés à des virus. Ce Guide référence N°4 reprend l'essentiel des dossiers et fiches pratiques dédiés à cette thématique. Il devrait vous aider à mieux comprendre les enjeux et vous permettre d'acquérir un premier niveau de défense. Entre le simple firewall et les suites complètes de sécurité très répandues, sont apparus des dizaines de nouveaux outils complémentaires, votre CD-Rom en contient un certain nombre. Mais les pirates qui cherchent surtout à récupérer des numéros de Cartes bleues et des plates-formes pour relayer leurs attaques font aussi évoluer leurs techniques. Ils s'installent, par exemple, de plus en plus discrètement sur les sites web pour mieux récupérer des informations personnelles monnayables. Car il ne faut pas se faire d'illusion, l'espace internet est une jungle dans laquelle il n'existe pas de droit unifié.

On n'arrive à un tel paroxysme dans le milieu informatique que l'envie de poursuivre les auteurs d'attaques est grande. À tel point que le Club européen de la sécurité a pu réunir à Paris une centaine des spécialistes autour d'un débat sur la « légitime défense numérique ». Pour les responsables sécurité, ce n'est plus simplement un virus qui les vise, c'est carrément leur poste et leur carrière professionnelle qui sont en jeu. À quoi bon pour des sociétés « s'offrir » un directeur de la sécurité si toute la firme peut être piratée et ses secrets de fabrication divulgués. D'où l'envie de ces responsables de « contre-attaquer » pour fournir, au moins, au-delà des traces des agressions, les adresses d'où proviennent les attaques. Mais cette « légitime défense numérique » est aussi une agression également condamnable d'où les conseils de la SGDN de ne pas se faire justice soi-même, mais de se confier à la police qui dispose d'un petit nombre de spécialistes. Pour les particuliers, sur son site www.securite-informatique.gouv.fr, les autorités préconisent une dizaine de bons commandements pour éviter d'être victime des virus avec au minimum des sauvegardes régulières. Le chantier de la sécurité n'est pas prêt d'être terminé.

Thierry Outrebon,
rédacteur en chef

« Les pirates qui cherchent essentiellement à récupérer des numéros de Cartes bleues et des plates-formes pour relayer leurs attaques font aussi évoluer leurs techniques. »

Release by TEAM-DZ

CD Windows news

Défendez votre ordinateur

CONFIGURATION REQUISE POUR UTILISER LES LOGICIELS DE VOTRE CD

- Windows, XP, Vista, W7
- Pentium IV minimum à 1,2 GHz
- 512 Mo de RAM
- DD de 250 Mo libre
- Éditeur : Ashampoo Winoptimizer 7
- Prix version d'évaluation valable 40 jours. Puis 39,99 € – 1 PC /1an
- Type de logiciel : Suite d'optimisation
- Occupe 26 Mo sur disque
- www.ashampoo. com/fr/eur

BON À SAVOIR

Attention aux doublons

Si vous disposez d'une version de Windows 7, vous disposez déjà d'un firewall. Dans le cas ou vous avez installé un second firewall, les temps de réponse seront allongés. Vous pouvez choisir de désinstaller celui qui vous conviendra le moins, avec le risque de perdre certaines infos d'administration. Attention le système le plus efficace et souvent le plus « filtrant » et donc le plus lent. Il vous faudra éviter d'effectuer deux fois les mêmes opérations. Les version les plus récentes sont en général les plus efficaces.

Au-delà des outils d'optimisation de votre PC, **il vous faudra protéger celui-ci des attaques incessantes venues du net.** Sans outils de sécurité, le temps passé à classer et nettoyer votre PC sera remis en cause.

Avast *La version 6 d'Avast prend en compte la sécurisation des navigateurs et un service antispam.*

La suite Security Essentials de Microsoft a eu pour effet de remonter le niveau moyen de tous les logiciels proposés sur le marché. Pour l'heure, la version proposée se distingue par une intégration facile à votre système d'exploitation. Beaucoup plus répandu que le logiciel de Microsoft en tant que logiciel libre Avast !Antivirus dans sa version 6.0 ne couvre qu'une facette des problèmes que l'on peut rencontrer. Pour Avast, ces versions gratuites sont aussi un moyen de faire la « courte échelle » aux versions payantes. Mais déjà la version la plus simple que nous vous proposons fait l'essentiel, c'est-à-dire qu'elle intègre un pare feu, un antivirus avec anti-espion, une interface SafeZone pour assurer la confidentialité de vos échanges financiers et protéger votre identité et vos données confidentielles.

Le courrier, un vecteur de virus important

Son antispam évitera que des courriers indésirables n'entrent dans votre boîte de courrier entrant. C'est d'ailleurs le domaine dans lequel, les virus prolifèrent de plus en plus, la navigation classique étant plus surveillée. Avec notre outil Spamihilator, vous devriez réduire sensiblement le nombre de fichiers suspects. Si vous êtes client Outlook, nous vous recommandons Spamfighter qui filtre les courriers malsains et vous évite les pièges du phishing. Cette plaie des messageries crée un véritable chemin de croix pour ceux qui ont commis l'erreur de répondre à des invitations frauduleuses. Vos enfants peuvent être en particulier sensibles aux tentations du web. Si votre opérateur n'en propose pas, Timeboss constitue une solution éprouvée en tant que logiciel de contrôle parental. Il vous permettra entre autres d'éviter les sites de racolage de jeux idiots. Parions néanmoins qu'après quelques années de pratique de votre PC, ils seront déjà capables de déjouer les contraintes de ce logiciel. Issu de développement sous Linux, Clam Antivirus, lui, n'est pas à la portée de tous les utilisateurs car il faut par exemple scanner les fichiers manuellement pour détecter un virus mais ses outils sont puissants en particulier ses outils d'analyses antivirus programmables. On apprécie la mise à jour automatique de la base de définitions de virus, un service en général payant ailleurs. Il s'intègre via son menu contextuel à Microsoft Windows Explorer et se présente comme un « greffon » de Microsoft Outlook. ■

Spamihilator *Si vous êtes victime d'un bombardement de publicité par mail ? L'installation de cet antispam réduit le volume des courriers inutiles.*

Release by TEAM-DZ

Optimisation, sécurité, dépannage

Nettoyage de printemps

Votre CD-Rom, ce mois-ci, contient une foule d'outils pour éliminer les fichiers inutiles et les éléments qui encombrent la base de registre. Autres sources de ralentissement, les fichiers épars de votre disque dur. Rangez-les.

> ASHAMPOO WINOPTIMIZER 7

Ashampoo WinOptimizer réunit au sein d'une même structure huit groupes d'utilitaires pour rafraîchir le système d'exploitation de votre PC. Comme la plupart de ces outils, il optimise la base de registre de Windows (Registry Cleaner) et efface les fichiers inutiles. Il scrute aussi les versions les plus récentes des fichiers DLL avec son DLL Cleaner. Généralement, il faut se méfier d'endommager « à la main » la base de registre qui est le cœur de l'OS, la moindre modification pouvant engendrer des blocages. On peut suivre facilement les opérations à effectuer. www..ashampoo.com/fr

> SYSTEM-MECHANIC

Ce logiciel de référence en est déjà à sa dixième version. Comme ses concurrents, il est le fruit d'une association d'une vingtaine d'outils différents qui peuvent néanmoins se classer en quatre groupes : l'optimisation, le nettoyage, la réparation et la sécurité. Ce dernier point est à souligner car, de plus en plus, les éditeurs de sécurité envahissent l'espace réservé jusque là aux outils d'optimisation de ce type. Dans ce domaine, System Mechanic, se distingue par un très bon outil de nettoyage de disque, qui permet aussi de défragmenter et d'établir un rapport sur l'état du disque ce qui est assez rare. www.iolo.com/system-mechanic

> DISKEEPER

La version 2011 de Diskeeper, lui aussi un must de l'optimisation du PC, dispose d'un mode « optimisé », c'est-à-dire une gestion quasi automatique des traitements de mise à jour en fonction des éléments qui posent problèmes. La défragmentation, en particulier est gérée immédiatement avec la fonction Instant Défrag qui analyse la façon dont les fichiers sont utilisés. Il défragmente immédiatement les plus utilisés. L'un des intérêts de Diskeeper 2011 est qu'il travaille en arrière-plan. Enfin un rapport de performances donne le statut de configuration du système. www.diskeeper.com

> PC TOOLS PERFORMANCE TOOLKIT

Il utilise un algorithme de détection pour identifier toute référence manquante ou invalide dans la base de registre. Le manque reste souvent lié à la suppression incomplète de logiciels, l'absence de pilotes de matériel ou encore la présence de programmes de démarrage orphelins. Il efface les traces de votre navigation. Le File Recover récupère les documents et autres fichiers importants effacés par mégarde. L'outil de gestion des performances surveille pour sa part l'utilisation du système, les processus, la mémoire et l'espace disque. www.pctools.com/fr/performance-toolkit

Release by TEAM-DZ

SÉCURISEZ VOTRE PC p.8

- **Sécurité : le guide des solutions ultimes** ... **p.8**
- Prenez la sécurité de Windows 7 en main p.13
- Astuces express p.18
- Contrôlez l'exécution des programmes p.19
- Un antivirus de secours : ClamAV p.21
- Sauvegardez sur mesure avec BackItUp 10 ... p.23
- Sauvegardez plus rapidement avec Rebit p.25
- Restaurez des données effacées p.27
- Échappez au crash du système d'exploitation . p.29
- Diagnostiquez votre ordinateur p.31
- Retrouvez vos fichiers disparus p.33
- Astuces express p.35

SÉCURISEZ VOTRE NAVIGATION p.36

- **Accédez plus vite à internet** **p.36**
- Astuces express p.44
- Sécurisez les droits d'accès à Facebook p.45
- Dopez Windows Mobile 6.5 avec Opera 10 ..... p.47
- Sécurisez Windows Live Essentials 2011 ..... p.49
- Installez le contrôle parental de SFR p.51
- Isolez le navigateur pour éviter les virus p.53

PROGRAMMEZ VOTRE SÉCURITÉ p.55

- **VBScript : Prenez le contrôle du système** ... **p.55**
- Administrez vos serveurs à distance p.60
- Créez la clé USB de la dernière chance p.67
- Détectez l'activité d'un bot depuis le réseau p.69
- Migrez vos données de communication p.71
- Prenez le contrôle d'un PC à distance p.73
- Sauvegardez vos données en réseau p.75
- Astuces express p.77

08 AUTREFOIS ŒUVRE DE QUELQUES «NERDS» EN QUÊTE DE RECONNAISSANCE, LES VIRUS, BOTNETS, SCAREWARES, CRIMEWARES, BREF, LES MALWARES, SONT DEVENUS LES ARMES DE GROUPES MAFIEUX, D'ACTIVISTES POLITIQUES OU RELIGIEUX, VOIRE MÊME LES MOYENS D'ATTAQUE ENVISAGÉS PAR LES ARMÉES MODERNES.

36 UN INTERNAUTE PEUT-IL ALLER PLUS VITE QUE CE QUE PEUT OFFRIR PAR DÉFAUT UN FOURNISSEUR D'ACCÈS? LA RÉPONSE EST OUI, À CONDITION DE FAIRE DES CHOIX ET CELA DÉPEND DU TYPE DE SERVICE UTILISÉ ET DU PRIX QUE L'ON PEUT Y CONSACRER.

55 DANS LA PANOPLIE DES OUTILS D'AUTOMATISATION DE WINDOWS, ON TROUVE LE LANGAGE VBSCRIPT. DIRECTEMENT DÉRIVÉS DE VISUAL BASIC, LES SCRIPTS VBS SONT DESTINÉS À AUTOMATISER CERTAINES TÂCHES, COMME LA COPIE DE FICHIERS OU LE CONTRÔLE DU NAVIGATEUR.

Release by TEAM-DZ

78 WINDOWS NEWS RÉPOND À VOS QUESTIONS ET ANALYSE LES PROBLÈMES QUE VOUS RENCONTREZ DANS L'USAGE QUOTIDIEN DE LA NOUVELLE VERSION DE WINDOWS.

92 COURTISÉES PAR LES VENDEURS D'OUTILS DE SÉCURITÉ, LES PME DOIVENT RECENSER LES PROBLÉMATIQUES AUXQUELLES ELLES SONT CONFRONTÉES. LES CHOIX S'AVÈRENT SOUVENT BASÉS SUR UN COMPROMIS. MAIS LES PROMESSES CHARMEUSES CACHENT SOUVENT DES LACUNES.

LE COIN DES BUGS p.78

- **CPU AMD & ventilation** **p.78**
- Maîtrisez les extinctions p.80
- Changez de look p.82
- Défragmentez le système p.84
- Des logos et des chaînes p.86
- Faites de la place p.88
- Raccourci pour cacher la Barre des tâches p.90

SÉCURISEZ VOTRE TPE p.92

- **Guide de sécurité pour votre PME** **p.92**
- La sécurité des PC nomades **p.98**
- Veillez sur vos stations de travail **p.104**
- Astuces express **p.108**

LE COURRIER DES LECTEURS p.109

- **Puis-je retirer la clé USB ?** **p.109**
- Les points de restauration disparaissent p.111
- Un port USB déficient p.115
- Scanner bloqué p.118
- Un soft à désinstaller p.122
- Le processeur sur le point de griller p.125
- Sauvegardez sans exporter p.128

109 JEAN-PAUL MESTERS, JOURNALISTE ET AUTEUR D'UNE TRENTAINE D'OUVRAGES D'INFORMATIQUE GRAND PUBLIC RÉPOND AUX QUESTIONS QUE VOUS VOUS POSEZ.

Release by TEAM-DZ

SÉCURITÉ LE GUIDE DES SOLUTIONS ULTIMES

Autrefois œuvre de quelques « nerds » en quête de reconnaissance, **les virus, botnets, scarewares, crimewares, bref, les malwares, sont devenus les armes de groupes mafieux,** d'activistes politiques ou religieux, voire même les moyens d'attaque envisagés par les armées modernes.

Le virus, ça n'existe pas. Du moins sous sa forme fantasmée, celle d'un programme unique de destruction universel. On devrait plutôt parler de « cocktail viral », savant assemblage d'éléments techniques très spécialisés, et dont le mariage aboutit à ce que l'on appelle un « malware ». Certains prennent le nom de « troyens » ou de « rootkits », d'autres encore de « spywares », ou alors d'e-mails de phishing susceptibles de conduire à une attaque « drive by download »… Ce sont là un jargon et des distinguos assez subtils qui, aux yeux des non-initiés, ne sont que prétextes inventés par les vendeurs d'antivirus et de coupe-feu. Reste que malgré ces multiples appellations et ces divers dangers , il est possible de dresser à grands traits un portrait-robot de ces outils d'attaque et d'infection.

Les trois redoutables armes du malware

Les logiciels destructeurs n'existent pratiquement plus de nos jours. Un « bon » virus est un virus qui ne casse pas sa machine cible et qui rapporte de l'argent… ne serait-ce que pour amortir ses coûts de développement et faire vivre toute l'organisation économique qui dépend de cette « industrie ». Or, ce qui rapporte le plus, dans notre monde dématérialisé, ce sont les informations : mots de passe et logon d'abonnement internet donnant accès aux fonctions de téléphonie IP illimitée, numéros de carte de crédit, crédences ouvrant des possibilités d'achat sur des sites marchands, documents personnels divers… Début juillet dernier, on a même découvert un botnet récupérateur de « certificats numériques ».
Pour s'emparer de ces trésors, le virus moderne doit à la fois pénétrer le périmètre de défense d'un ordinateur (son firewall, son antivirus, ses mécanismes antispyware et antiphishing, etc), puis y déposer une « charge utile » - l'outil de récupération de données proprement dit - et enfin communiquer avec l'extérieur, soit pour y expédier le fruit des recherches, soit pour laisser pénétrer d'autres « charges utiles » plus perfectionnées. Car les virus sont également capables de se « mettre à jour », tant pour éviter d'être détectés par les antivirus qui eux aussi évoluent en fonction des menaces, que pour

Release by TEAM-DZ

se protéger d'autres virus qui ne supportent pas la présence de leurs frères d'infection.

Les tactiques des auteurs de virus les plus dangereux

Ces trois étapes que suivent les malwares sont de natures très différentes. La première partie, le système de pénétration à proprement parler, fait l'objet chaque jour de nouvelles découvertes et publications. La moindre faiblesse d'un système d'exploitation (Windows notamment) ou d'un logiciel très répandu - Acrobat Reader, Flash Player…- est immédiatement décortiquée afin de savoir s'il est envisageable de l'exploiter à distance. On trouve dans cette catégorie une foultitude de moyens : fausses URL appelant un exécutable, injection

Chiffres | Le hit parade des malwares

LA CÔTE DES ÉDITEURS Ce tableau - qui ne recense pas les attaques, mais les « défauts officiellement recensés » - reflète relativement fidèlement à la fois l'intérêt que ces logiciels éveillent chez les auteurs de malwares, et l'attention soudaine que l'éditeur porte à la sécurisation de ses productions. On voit très clairement la « montée en puissance » du renforcement de produits tels que VMware, Acrobat Reader, Oracle (application et SGBD) et Apple, qui persiste à entretenir une image de « produit invulnérable ». On remarque également l'efficacité de la « prime à la découverte de bug » de Mozilla.

Release by TEAM-DZ

de données non conformes dans un formulaire (une URL de site web ou un champ de « logon » de plus de 256 caractères par exemple), pseudo-applications Java ou faux codecs audio et vidéo, fichiers d'aide « forgés » (c'est-à-dire dont la structure ou le contenu ont été modifiés)… Certaines techniques (dic by download, fichiers multimédias infectés, DNS spoofing conduisant vers un faux site, voir encadré « Jargon des attaques ») tirent même parti des failles situées « dans le cerveau de l'utilisateur » pour qu'il télécharge lui-même le code d'attaque et lui fasse franchir les défenses périmétriques de sa propre machine. Cela consiste par exemple à lui demander de télécharger une mise à jour de logiciel ou une « applet » de navigateur qui en fait ne sont que des codes malicieux déguisés. Toujours dans le même registre, découvrir une faille et le moyen de l'exploiter rapporte également beaucoup d'argent à son auteur. À l'heure actuelle, Google, la fondation Mozilla et le Zero Day Initiative vont jusqu'à payer près de 3 000 euros tout découvreur - on parle d'inventeur - de faille importante et inédite. Et ce ne sont là que les tarifs officiels pratiqués par des entreprises soucieuses de la sécurité de leurs clients… Au marché noir, un bel « exploit » (dans le sens de méthode de pénétration à distance) peut dépasser 5 à 6000 euros. Des tarifs qui vont d'ailleurs croissant au fur et à mesure que les éditeurs - Microsoft, Cisco, Adobe et Apple en tête - colmatent leurs failles et consolident leurs défenses.

Zoom | Les différents types de malware

LES VIRUS, UN VIEUX CLASSIQUE C'est la plus connue des nuisances informatiques. Un « bon » virus est capable de s'introduire dans un ordinateur, de se dupliquer, de se répandre, et d'effectuer un acte soit destructeur, soit malveillant (vol d'information, ouverture de portes dérobées, destruction de programmes, chiffrement d'informations à des fins de racket…). Ses différentes formes, ses évolutions (ver ou « worm », troyens…) ne sont que des variations sur ce même thème: tous font mal, tous sont dangereux, tous évoluent.

LE SPAM, LES ADWARES, LE CYBER PORTE-À-PORTE Le spam, ce sont ces tonnes de courriels pouvant tout aussi bien vanter les mérites d'un fortifiant sexuel que les dernières promotions d'un vendeur de matériel informatique: le spam des uns, c'est la publicité des autres. Idem pour les « adwares », ces programmes intrusifs qui affichent des publicités intempestives sur l'écran de la victime. Plus « douces », les réclames qui se basent sur le profil de vos dernières consultations (Google et Amazon sont des spécialistes du genre).

LES SPYWARES, LES ROOTKITS On entre dans la catégorie « high tech » des outils criminels, qui se cachent pour espionner sans se faire remarquer. Les techniques de virtualisation, de plus en plus courantes, facilitent la prolifération de certains de ces codes (voir les recherches de Joanna Rutkowska sur le sujet). Cette tendance est contrebalancée par la généralisation des programmes « signés » et authentifiés par le système d'exploitation.

LES SCAREWARES On entre là dans le domaine de la guerre psychologique, puisque le scareware, ou « faux antivirus », se fait passer pour un logiciel « légal et authentique », avec un prix fixe (entre 40 et 90 euros), un réseau de distribution réel, des logos et un aspect rappelant ceux des véritables programmes. Certains scarewares se doublent de programme de chiffrement-prise en otage de données, « libérées-déchiffrées après payement d'une rançon » (racketiciel).

LES CRIMEWARES, PHISHING, SCAM ET AUTRES ATTAQUES HUMAINES L'un des maillons les plus aisément attaquables est l'esprit humain. Deux doigts d'alarmisme, et un employé modèle peut fournir logon, mot de passe, numéro de carte de crédit, date de naissance, adresse complète à un prétendu correspondant « chargé de la sécurité de l'entreprise » ou à une veuve éplorée de général africain décédé… et milliardaire. Même de très suspicieux responsables d'agences bancaires se sont fait prendre à ce jeu. Contre ces menaces, les filtres antispam et les mécanismes de blocage de sites de phishing apportent une réponse trop partielle: il n'existe pas de « firewall » adapté au cerveau humain.

Des malwares quasiment invisibles

Les deux autres armes - charge utile et communication des données - sont d'une nature nettement moins technique et rapportent bien moins à leurs auteurs. Elles exigent toutefois une certaine subtilité dans l'écriture et une maîtrise absolue des environnements d'exécution. La charge utile, par exemple, doit pouvoir s'exécuter sans que le noyau de Windows ne détecte une activité suspecte, tout en faisant croire à l'antivirus que le processus en question fait partie du système d'exploitation. Certaines charges prennent le nom et l'apparence d'une DLL ou d'un EXE « système », d'autres se cachent dans des machines virtuelles, d'autres encore se logent dans des recoins de la mémoire situés en deçà des zones contrôlées par le système - et donc par l'antivirus. Restent les fonctions de communication. C'est paradoxalement l'un des outils qui a longtemps été l'un des plus simples à concevoir, puisque la majorité des firewalls étaient conçus pour interdire les communications « entrantes » sans s'occuper des canaux « sortants ». Les choses évoluent dans le bon sens depuis trois ou quatre ans. Hélas, les auteurs de malwares ont de plus en plus souvent recours à des moyens de communication chiffrés (VPN par exemple), fragmentés ou agiles (le virus peut changer de protocole). Ils détournent même à leur profit les voies utilisées par le propriétaire de l'ordinateur (Messenger, client P2P, etc.).

Boîte à outils pour truand binaire

Outre ces trois fonctions de « base », il faut ajouter toute une série d'outils et de méthodes encore plus techniques, qui permettent au virus de survivre dans un environnement hostile. À commencer par un système d'autoreproduction. Non

Release by TEAM-DZ

seulement il donne au virus la possibilité de se dupliquer et d'étendre son emprise sur plusieurs systèmes, mais en outre cette fonction lui permet de se cloner rapidement - tant en mémoire que sur les disques ou clés USB - pour résister aux assauts d'un logiciel de protection. Une armée capable de produire plus de soldats que ne peut en aligner l'ennemi est une armée invincible… tant que l'ennemi en question n'a pas découvert le moyen de bloquer ce processus de reproduction.

Les malwares reconnaissent leur environnement

Cette fonction ne doit pas être confondue avec celles plus spécifiques liées à la diffusion de l'infection. Car une fois dupliqué, le malware doit être capable de détecter un moyen de communication - liaison bluetooth, brin réseau Wi-Fi ou cuivre, lien FTP, détection de ressource USB - non plus pour expédier les données qu'il aura récupéré, mais pour étendre son royaume et s'ouvrir de nouveaux horizons… Certains virus intègrent même de véritables serveurs de messagerie pouvant vampiriser le carnet d'adresses de leur première victime et envahir le monde de proche en proche. Viennent ensuite les outils en activité permanente, déjà mentionnés au fil du paragraphe précédent. Ce sont principalement des mécanismes de mise à jour qui effectuent des « updates » de virus et assurent son adaptation aux menaces diverses. Proches cousins des outils de permanence, les armes d'attaque et de défense. Les principaux « botnets » (réseaux de machines « zombifiées » par certains virus spécifiques) en possèdent toute une panoplie : accessoires de désactivation d'antivirus ou de détournement des canaux de mise à jour automatique, antivirus spécifique destiné à combattre d'autres virus du même type, changement de techniques d'attaques en cas de parade de la part d'un programme de protection… Une branche très spécifique des outils de défense, l'art du camouflage, parachève cette longue liste. Le camouflage consiste généralement à faire en sorte que le virus puisse changer d'aspect et ainsi échapper à toute reconnaissance de « signature ». Une part croissante des virus modernes sont « polymorphes », c'est-à-dire que chaque infection montre un poids binaire différent de sa voisine. En outre, ces programmes sont eux-mêmes chiffrés, rendant impossible toute analyse, et doublés de fonctions de furtivité. Qu'un antivirus tente d'analyser un programme infecté, et le virus immédiatement présentera au scanner l'image du fichier tel qu'il était avant l'infection, ou s'extraira lui-même du fichier le temps de l'analyse.

Quelle charge utile ?

REPÈRES…

> L'IMPACT ECONOMIQUE La nature de la charge utile est souvent riche d'enseignements. Ainsi, la campagne de vol d'informations qui a frappé, au premier trimestre 2010, les sociétés Google China, Adobe et certains groupes pétroliers américains a montré qu'il existait de plus en plus de « virus d'espionnage industriel ». Ce n'est pas la première fois que l'on détecte des détournements massifs de fichiers pdf, doc, txt, xls et autres, généralement vers ce qui semble être des ordinateurs situés en Chine. Les réseaux de bot - botnet, ou réseaux de machines « zombifiées » effectuant discrètement des opérations illégales à l'insu de leurs propriétaires - sont également légion au sein des entreprises. Cette forme « d'abus de bien social » peut également constituer un canal d'accès à d'autres fuites d'information. Reste enfin la « charge utile » la plus répandue : le récupérateur de mots de passe et de crédences bancaires. Ces malwares sont à la base de toute l'organisation financière des réseaux mafieux.

> Un rootkit va s'installer en cliquant sur « No ». Difficile de ne pas tomber dans le piège.

Un cocktail détonant : agitez et servez chaud

Est-il nécessaire de préciser que, de plus en plus, les auteurs de malwares se spécialisent ? Chaque outil ou arme devenant de plus en plus élaboré, il y a, chez les auteurs de virus, des spécialistes du camouflage, des experts en exploitation de faille, des gourous des techniques de propagation et de duplication, des seigneurs du contournement antiviral… Mais alors, les propagateurs de virus doivent avoir un carnet d'adresse impressionnant pour arriver un jour à « pondre » une infection efficace ? C'est effectivement le cas pour certains. Mais là encore, la parcellisation et la professionnalisation des Black Hats crée de nouvelles structures organisationnelles. Et si certains auteurs travaillent « encore » en équipe, d'autres échangent et vendent leurs développements sur des places de marché virtuelles, sur internet. On écrit désormais un virus un peu comme l'on confectionne un potage, en associant des poireaux d'intrusion, des carottes d'autoréplication, des navets de camouflage. Pis encore, il existe, pour les non spécialistes, des automates de fabrication de virus qui vont piocher dans une bibliothèque des fonctions de base choisies à l'aide d'un menu à choix multiple, avec une séduisante interface graphique. Peu étonnant dans de telles conditions de découvrir des potages relativement mortels,

JARGON

Exploit Utilisation active d'un défaut de conception (faille) découvert dans un logiciel.
BoF (Buffer Overflow) Attaque par saturation d'un tampon mémoire (généralement un champ de saisie) qui peut donner accès à la mémoire vive de l'ordinateur victime.
MiM (Man in the Middle) Interposition d'un élément entre un poste client et un serveur.
XSS (Cross Site Scripting) Terme générique désignant l'exploitation d'une vulnérabilité sur un serveur web et servant à « injecter » un malware sur les postes des visiteurs.
DoS Denial of Service Déni de service. Attaque incapacitante visant à affecter le comportement d'un serveur ou d'un poste. Généralement utilisé par les spécialistes de l'escroquerie à la rançon.
Backdoor (porte dérobée) Ouverture d'un canal de communication destiné soit à exfiltrer des données confidentielles, soit à faciliter une intrusion, directe, soit à « mettre à jour » la charge utile.

Release by TEAM-DZ

LA FRONTIERE ENTRE LES OUTILS DE MARKETING ET LES VIRUS DES BANDES MAFIEUSES **TEND À S'AMENUISER, L'INFO « PRÉCISE » RESTANT LA CIBLE COMMUNE.**

ACHAT

40 euros, c'est le prix moyen d'une licence antivirus officielle. C'est aussi celui d'un « scareware », qui imite jusqu'au tarif des vrais outils. En préambule, un mail avertit lourdement l'utilisateur que sa machine est infectée, pour le contraindre à se procurer ce type de solution inefficace.

avec parfois deux ou trois méthodes d'intrusions différentes, tout autant de charges utiles, une foultitude de moyens de propagation et de communication, des options de polymorphisme… ces outils de fabrication de malwares sont vendus « à la licence », parfois même bridés en quantité, avec un service après-vente, une garantie de mise à jour. On peut ainsi louer un botnet qui servira de réseau de première diffusion, acheter des fichiers de clients « cible » si l'on vise un secteur très particulier de l'industrie, louer les services de « revendeurs » payés à la commission en fonction du chiffre d'affaire réalisé... C'est ainsi que fonctionne le business des faux-antivirus, également appelés Scarewares. Paradoxalement, on retrouve des techniques d'intrusion, d'installation silencieuse, voire d'attaque psychologique visant l'utilisateur dans des programmes théoriquement inoffensifs et officiellement diffusés. C'est notamment le cas des BHO (Browser Helper Objects), ces accessoires qui viennent prétendument enrichir la pratique d'un navigateur internet. Parmi eux, certains « spywares commerciaux », ou outils de conseil marketing, voire même des logiciels destinés à lutter contre le piratage (ainsi un malheureux programme de DRM diffusé sur certaines productions de Sony Music, ou, plus récemment, un logiciel de filtrage Hadopi brièvement commercialisé par Orange). Ces programmes sont non seulement parfois installés à l'insu des usagers, mais en outre comportent eux-mêmes des failles qui pourraient fort bien les transformer en vecteurs d'infection.

Car la tentation est grande de « retourner » un logiciel ou un matériel largement diffusé pour en faire un vecteur d'intrusion planétaire. Déjà, les messageries instantanées, les softphones VoIP, certains réseaux sociaux, les espaces de commentaires des blogs ont été exploités par des personnes mal intentionnées. Le monde de la téléphonie, qui se concentre sur trois ou quatre OS, a peu de chances d'être épargné.

Une nouvelle menace: les malwares d'État

S'ajoute à ce tableau un nouveau décor, probablement plus orwelien: celui des malwares d'État ou d'organisations politiques, voire d'intérêts industriels. Ceux-là sont, pour certains, ignorés des antivirus, inconnus des firewalls, lorsque ce n'est pas l'antivirus ou le firewall lui-même qui en protège la présence. Trois exemples concrets: mi-juin 2010, les éditeurs de l'antivirus Virus BlokAda découvrent l'existence d'un certain Trojan-Spy.0485 exploitant la faille MS10-046 dite « faille lnk ». Le programme cherche à s'introduire au cœur d'un logiciel Siemens spécialisé dans la gestion des processus industriels. Premiers visés: les fournisseurs d'énergie, les gestionnaires d'infrastructures nationales de flux. Les réglementations des États-Unis imposées par le DHS (Département de la Sécurité intérieure) imposent aux équipementiers d'outils de télécommunication, du routeur à l'autocommutateur téléphonique, de posséder un « point d'entrée » permettant aux autorités d'avoir accès au flux en transit. La France possède elle-même un catalogue des firewalls, VPN, routeurs de fabrication nationale dont l'usage est « conseillé ». Ce qui signifie que si cet équipement est probablement protégé contre les écoutes américaines, il est sans le moindre doute ouvert à celles des services de renseignements nationaux. On appelle cela une « clé de séquestre », et c'est on ne peut plus légal. Reste à espérer qu'aucun truand ne percera ce genre de secret! ■

Focus | Le prix d'un botnet

■ ECONOMIE UNDERGROUND

Combien pour un botnet diffuseur de spam, de malwares « ciblés » ou générateur d'attaque en déni de service? Moins cher qu'un service équivalent (mais légal) commercialisé par un Amazon ou un Google. En début d'année, la société Verisign, après avoir enquêté sur les tarifs des vingt-cinq plus gros « botnet herders » (gardiens de botnets), publiait une étude estimant à $ 8,94 le coût horaire d'une telle location. Soit 67 dollars la journée avec tarif dégressif à la clé. Les opérations (attaque d'un site, diffusion de spam, inondation de « bannières publicitaires ») sont tarifées avec rigueur et précision. La facture peut augmenter si l'on désire affiner la cible (clients spécifiquement français, victimes anglophones ou germanophones, etc.), mais les prix demeurent à la portée d'un petit truand de quartier ou d'un concurrent jaloux. Contrairement à une croyance populaire, il existe pratiquement autant de machines compromises situées au sein des entreprises que chez les particuliers.

Release by TEAM-DZ

Prenez la sécurité de Windows 7 en main

Même si Windows 7 est l'OS le plus sécurisé de Microsoft, il n'en reste pas moins qu'**une bonne maîtrise de son paramétrage est nécessaire**. Voici comment dompter le pare-feu, l'UAC et le 64 bits et comprendre comment fonctionne tous les éléments de sécurité.

NIVEAU
Confirmé

MATÉRIEL NÉCESSAIRE
- Windows 7
- Runasspc (http://robotronic.de/runasspcEn.html)

TEMPS DE RÉALISATION
60 minutes

La sécurisation de Windows 7 passe par de nouvelles habitudes, comme l'utilisation d'un compte utilisateur et l'activation du contrôle de compte (UAC). C'est aussi l'occasion de passer au 64 bits. Dans ce mode, l'OS de Microsoft propose plusieurs mécanismes de sécurité qui ne sont pas valables en 32 bits. Mais avant de nous intéresser à toutes les mesures à mettre en place, il faut revenir sur les différents mécanismes de sécurité présents dans Windows 7.

Apprenez à bien gérer les droits utilisateurs

Dans tous les systèmes d'exploitation modernes, la première défense contre les malwares et les tentatives d'intrusion prend la forme d'un système de gestion des droits. On le trouve à deux niveaux : sur les fichiers et dans les actions qui peuvent être entreprises. Sous Windows 7, on trouve deux profils prédéfinis accessibles aux utilisateurs : l'administrateur et l'utilisateur standard. Le système possède, lui, différents « utilisateurs », comme le système, le service réseau, le service local ou encore TrustedInstaller. L'ensemble de ces utilisateurs a des droits d'accès à certains fichiers et dispose d'un cadre bien défini pour interagir avec d'autres programmes ou paramètres. Les programmes fonctionnant à travers le navigateur web n'ont par exemple pas le droit d'écrire ailleurs que dans des répertoires définis et ne peuvent accéder qu'à une partie très limitée de la Base de registre. Cette gestion des droits permet de différencier les accès par utilisateurs et donc de protéger certains documents ou éléments du système. C'est aussi un très bon moyen pour éviter que des malwares ne modifient les fichiers du système et s'installent durablement dans ce dernier… À moins qu'un utilisateur administrateur ne leur donne le droit de s'exécuter. Dans ce cas-là, le programme malveillant récupère les droits du profil et peut engager toutes les actions qu'il souhaite. C'est donc ici que commence le bon paramétrage d'un poste : il est impératif, dans l'usage quotidien, de ne pas utiliser un compte

SOMMAIRE

p.14
LES OUTILS INDISPENSABLES
Évitez les virus grâce à Secunia PSI, Malwarebytes' et Web Of Trust.

p.14
GÉREZ LE MODE UTILISATEUR
Créez des comptes limités pour ne plus mettre en péril votre système.

p.15
TPM ET BITLOCKER À LA RESCOUSSE
Ils luttent contre les malwares s'attaquant à Windows 7 en 64 bits.

p.16
LES DIFFÉRENTES ALERTES WINDOWS
Sachez quel logiciel ou quelle action a déclenché une alerte de l'UAC.

p.17
GÉREZ LES ACCÈS AUX DOCUMENTS
Choisissez les utilisateurs avec lesquels vous voulez partager des répertoires.

Release by TEAM-DZ

Pratique | Les applications indispensables

> SECUNIA PSI Ce logiciel liste régulièrement les applications installées sur votre PC. Cette liste est ensuite croisée avec celle des vulnérabilités connues qui permettraient à un malware de s'introduire dans votre ordinateur. Le logiciel donne alors le lien pour télécharger le correctif proposé par l'éditeur.

> MALWAREBYTE'S ANTIMALWARE Cette application est conçue pour traquer et supprimer d'éventuels malwares qui seraient présents sur votre ordinateur. Même s'il ne dispense pas d'un antivirus, ce logiciel est d'un grand secours contre les malwares les plus tenaces.

> WOT Il est primordial de savoir si vous pouvez faire confiance aux sites web que vous visitez et sur lesquels vous téléchargez. Web of Trust (**www.mywot.com**) est l'un des systèmes gratuits pour établir la « réputation » de sites. D'autres existent, comme **www.siteadvisor.com** ou **safeweb.norton.com**.

administrateur. Lors de l'installation de Windows 7, le premier utilisateur créé est administrateur. Vous pourrez le transformer en utilisateur standard en créant un second administrateur (voir notre pas à pas ci-dessous). Cette opération est à entreprendre une fois que vous aurez installé les pilotes et les programmes que vous souhaitez utiliser. Si vous comptez plusieurs utilisateurs sur votre poste, vous pourrez aussi endencher le contrôle parental afin de limiter les possibilités d'installation de logiciels. Pour ce faire, rendez-vous dans *Panneau de configuration > Comptes et protection des utilisateurs >Contrôle parental*. Sélectionnez *Activé* puis cliquez sur *Autorisez et bloquez des programmes spécifiques*. Vous pourrez alors limiter les programmes que l'utilisateur pourra lancer dans sa session. À cette première protection s'est ajouté, depuis Windows Vista, le contrôle de compte utilisateur (ou UAC pour User Account Control). Microsoft ayant constaté que la plupart des usagers exploitaient leur ordinateur avec un profil administrateur, l'éditeur a créé un « filet » en ne donnant que des droits partiels d'administration à ce profil par défaut. Il affiche pour cela un message d'avertissement dès que l'action ou le programme lancé veut accéder à des éléments essentiels du système.

Comprennez l'UAC et sachez bien réagir

Le contrôle de compte utilisateur apparu avec Windows Vista a été aménagé dans Windows 7. Il comporte quatre niveaux d'alerte. Vous pouvez y accéder en tapant *contrôle de compte* dans le champ *Recherche* du menu *Démarrer* de Windows. Par défaut, il est au niveau 3 pour l'administrateur et 4 pour les utilisateurs restreints. Le nouveau niveau (2) a le même degré de sécurité que le 3 mais n'estompe pas le bureau (ce paramètre n'est utile que sur une petite configuration). Dans l'optique d'améliorer la sécurité d'un poste, il convient de ne pas désactiver ce mécanisme (niveau 1). L'UAC a une fonction essentielle dans la sécurité de Windows : elle permet de détecter tous les programmes qui nécessitent une élévation de privilège pour fonctionner. Faut-il s'alarmer d'une alerte ? Non, car elles sont normales dès lors que

Pas à pas | Gérez le mode utilisateur

1 CRÉEZ UN AUTRE ADMINISTRATEUR Dans le menu *Démarrer* de Windows, tapez *créer un compte* et choisissez *Créer un compte administrateur*. cochez *Administrateur* dans la fenêtre qui s'ouvre et indiquez un nom. Cliquez sur ce compte puis sur *Créer un mot de passe*.

2 MIGREZ L'ADMINISTRATEUR Dans *Panneau de configuration > Comptes et protection des utilisateurs > Comptes d'utilisateurs > Gérer les comptes*, sélectionnez votre compte puis cliquez sur *Modifier le type de compte*. Choisissez *Utilisateur standard*.

3 LES PROGRAMMES DU DÉMARRAGE (1) Une fois le changement de profil effectué, certains programmes du démarrage font apparaître une alerte à chaque lancement du PC : ils doivent être exécutés en mode Administrateur pour fonctionner correctement.

Release by TEAM-DZ

TECHNIQUE

TPM et BitLocker à la rescousse

> 64 BITS Même s'il est très difficile de modifier le noyau de Windows en mode 64 bits, plusieurs hackeurs ont conçu une procédure qui permet de le faire et qui a été depuis reprise dans plusieurs malwares (Alureon). L'astuce consiste à modifier le secteur de démarrage du disque dur (Master Boot Record) et de le renvoyer directement sur le malware. Ce dernier va alors cacher les éléments du malware aux « yeux » du système et de l'utilisateur. Pour parer à ce type d'infection, il n'existe qu'un seul moyen : l'utilisateur d'une « chaîne de confiance ». Elle nécessite la présence d'un module TPM (Trusted Platform Module) et l'emploi de BitLocker. Le premier va permettre de certifier l'authenticité des différents éléments logiciels du système. Ainsi, la modification du MBR empêchera le démarrage de Windows et interdira l'action des malwares « rootkit » utilisant cette brèche.

l'utilisateur interagit avec l'ordinateur. L'important est de bien identifier quel programme ou quelle action a déclenché une alerte de l'UAC. Dans le détail, vous trouverez, dans le pas à pas page 16, les éléments qu'il faut observer pour bien comprendre ces informations. L'UAC stoppant l'exécution d'un programme si vous répondez *Non* à une requête, il permet de bloquer des codes potentiellement dangereux. Reste à les reconnaître… et c'est tout le problème pour l'utilisateur. S'il s'agit d'un programme téléchargé sur le web, il doit provenir du site de son auteur ou d'un site de téléchargement connu (Clubic, download.com…). Au moindre doute, utilisez le site de dépistage des malwares, virustotal.com pour soumettre l'exécutable aux différents moteurs antivirus de ce site. L'UAC est d'autant plus essentiel qu'il est relativement difficile à contourner. Il utilise notamment un mode vidéo spécial qui empêche toute modification du message affiché (et qui pourrait tromper l'utilisateur). C'est donc une arme essentielle dans la sécurité de Windows 7. D'autres mécanismes œuvrent plus discrètement.

ASLR, DEP et Patchguard : les gardiens de votre mémoire

L'ASLR (pour Address Space Layout Randomization) est un procédé de gestion de la mémoire. Lorsqu'il est utilisé par un programme, les adresses-mémoires qui vont lui être allouées sont choisies de manière aléatoire. Ce procédé permet d'éviter que des malwares n'utilisent des applications courantes en s'attaquant à leurs éléments en mémoire. En effet, par défaut, certains processus s'exécutent toujours dans les mêmes adresses-mémoires. Le second mécanisme, DEP (pour Data Execution Prevention) vise à lutter contre l'exploitation de failles de sécurité par « dépassement de tampon-mémoire ». Ce type d'erreur de programmation est très courant. Lorsque des données extérieures au programme sont entrées, le programmeur doit écrire un mécanisme de vérification pour que la saisie ne dépasse pas la taille de la mémoire allouée à ces données. Si ce mécanisme est défaillant et que des données dépassent le « tampon-mémoire », le processeur les exécutera sans restriction. Les malwares utilisent à outrance ce procédé. DEP est donc là pour interdire l'exécution de toutes données qui dépasseraient les adresses-mémoires allouées à un programme. DEP est activé par défaut pour tous les programmes fonctionnant en 64 bits. Dernier mécanisme de protection : Patchguard. Ce dernier n'est présent que sur les versions 64 bits de Windows (Vista et 7). Il protège spécifiquement les fichiers du noyau de Windows contre d'éventuelles modifications et le détournement de ressources matérielles par des rootkits. Ces trois éléments agissent indépendamment de l'utilisateur, mais peuvent être activés avec un outil appelé EMET. Il s'agit d'un utilitaire proposé par Microsoft afin d'activer les fonctions DEP et ASLR pour certains programmes qui n'utilisent pas ces mécanismes. Cela permet de sécuriser des processus (notamment les plug-ins du navigateur), au cas où ces derniers n'auraient pas activé ces éléments. Vous pouvez récupérer gratuitement EMET à l'adresse http://tinyurl.com/emetversion2. Il suffit de cliquer sur Configure app pour ajouter

L'ASTUCE

BAS LES MASQUES !

Certains fichiers de malware cachent leur aspect « exécutable » en se faisant passer pour des documents Word (ou autre). Leur véritable extension est cachée par Windows. Pour savoir ce qu'il se cache derrière chaque fichier, vous devez visualiser la véritable extension du fichier. Ouvrez un répertoire quelconque puis cliquez sur *Organiser* et sélectionnez *Options des dossiers*. Dans l'onglet *Affichage* décochez *Masquer les extensions de fichier dont le type est connu*. Vous pouvez aussi faire apparaître les fichiers du système et les dossiers cachés.

4 LES PROGRAMMES DU DÉMARRAGE (2)
Ouvrez une console (menu *Démarrer > rechercher > cmd.exe*). Placez-vous dans le répertoire du logiciel runasspc. Ce programme va créer un fichier crypté avec vos identifiants administrateur et le programme à lancer.

5 PROGRAMME EN ADMINISTRATEUR (1)
Personnalisez la commande *runasspc/cryptfile:"crypt.spc"/program:"prog.exe"/domain:"localhost"/user:"admin"/password:"pass"*. *Prog.exe* est le programme à exécuter en mode administrateur, *Admin* le nom à utiliser.

6 PROGRAMME EN ADMINISTRATEUR (2)
Créez un fichier et inscrivez-y *c:\repertoirederunasspc\runasspc.exe /cryptfile:""crypt.spc""/quiet*. Renommez le en .bat et copiez-le dans *c:\Users\votreuser \AppData\Roaming\Microsoft\Windows\Start*Menu\Programs\Startup.

Release by TEAM-DZ

un programme et lui imposer l'utilisateur de DEP et ASLR.

Mode 64 bits : le choix de la sécurité

La sécurité est aussi une question de choix lors de l'installation de Windows 7. Sa version 64 bits possède plusieurs systèmes de sécurité qui ne sont pas présents en 32 bits. On trouve tout d'abord Patchguard, dont nous parlions plus haut. Certes, il existe des moyens de contourner Patchguard, mais il faut alors s'attaquer au démarrage de Windows, notamment au secteur de boot du système (voir notre encadré sur Bitlocker et les modules TPM). Cette protection rend plus complexe la réalisation de rootkits car ces derniers doivent interagir avec des éléments clés de Windows pour pouvoir se cacher correctement. Second élément de sécurité, tous les programmes tournant en 64 bits utilisent DEP. Cette protection évite donc l'exploitation de failles de sécurité non corrigées. Autre élément limitant les malwares, les pilotes de périphériques doivent obligatoirement être signés pour pouvoir s'installer sur un système 64 bits. Là aussi, les rootkits peuvent être bloqués dans leur attaque dès lors que l'utilisateur administrateur répond correctement aux demandes du système. L'installation d'un pilote déclenche une alerte de l'UAC, alerte qui doit être bien lue pour savoir qui demande cette installation et ce qu'elle va réellement installer. Cette protection reste toute relative : pour quelques dizaines de dollars, il est possible de se payer un certificat. Cependant, l'autorité de certification est censée identifier la personne qui a déposé ce certificat, ce qui devrait freiner les ardeurs des malfrats. Enfin, et c'est là une des raisons les plus intéressantes d'utiliser le mode 64 bits : les systèmes 64 bits étant encore peu nombreux, les auteurs de malwares n'ont pas encore développé de code pour cette plate-forme. La quasi-totalité des virus ne fonctionne tout simplement pas dans cet environnement.

LA VERSION 64 BITS DE WINDOWS 7 POSSÈDE **PLUSIEURS SYSTÈMES DE SÉCURITÉ QUI NE SONT PAS PRÉSENTS** EN 32 BITS.

Le gestionnaire de pare-feu avancé de Windows permet de créer des règles par application et de bloquer le trafic sortant.

64 bits : attention à la mise en place

Le choix d'un système 64 bits nécessite cependant plusieurs précautions, car certains éléments matériels ou logiciels peuvent s'avérer incompatibles. Côté matériel, il faut d'abord s'assurer que le constructeur des périphériques de votre machine a bien développé un pilote compatible. Microsoft propose un « conseiller de mise à niveau ». Ce programme téléchargeable sur http://windows.microsoft.com/fr-FR/windows/downloads/upgrade-advisor va inspecter votre machine et déterminer si des éléments peuvent être incompatibles. Un rapport d'analyse spécifique à la version 64 bits est disponible. Le second élément à prendre en compte concerne la migration vers Windows 7 en version 64 bits : impossible de conserver ses applications telles quelles. Vous devrez impérativement réinstaller tous vos logiciels. Par contre, ces derniers pourront ne pas fonctionner en 64 bits : le système saura quand même les faire tourner.

Windows Defender contre les malwares

Windows n'est pas non plus totalement démuni contre les malwares qui auraient réussi à s'installer. La mémoire et les fichiers sont régulièrement scannés par le module Windows Defender. Ce dernier fonctionne sur la base de signatures que Microsoft met régulièrement à jour via Windows Update. Vous pourrez y accéder en tapant *Windows defender* dans le champ *Recherche* du menu *Démarrer*. Rendez-vous dans l'onglet *Historique* pour vérifier qu'aucun indésirable n'a déjà été détecté. Vous pourrez ensuite lancer une analyse dans l'onglet *Analyser*. Cet outil est efficace pour détecter et supprimer

Pas à pas | Les différentes alertes Windows

1 ALERTES PROGRAMMES À la suite du téléchargement d'un programme et si celui-ci ne comporte aucune signature numérique, l'UAC affiche une alerte précisant le nom du programme et son origine. Ces fichiers doivent être vérifiés par un antivirus.

2 ALERTES DE MODIFICATION DU SYSTÈME Lorsqu'un programme s'installe ou que l'utilisateur modifie des paramètres du système, une alerte indique le nom du programme et de son éditeur. Vérifiez bien que ces éléments correspondent à l'action en cours.

3 ALERTES « PILOTE » Lors d'une installation, une alerte peut apparaître si le programme tente de mettre en place un pilote sans signature numérique valide. Si ce n'est pas un installeur de matériel, il y a des chances que ce soit un malware, car peu de logiciels nécessitent ces éléments.

Release by TEAM-DZ

les virus les plus courants. Cependant, un véritable antivirus sera plus à même d'assurer une bonne protection même si cette option reste facultative, dans la mesure où l'utilisateur gère correctement les téléchargements et les logiciels qui sont lancés sur son ordinateur (vérification de la réputation des sites et utilisation de www.virustotal.com pour tous les exécutables téléchargés).

Le pare-feu pour protéger votre réseau

La sécurité de Windows 7 n'est évidemment pas présente qu'en local, elle concerne aussi le réseau. Ce dernier fonctionne à partir de profils de règles suivant le type de réseau auquel votre ordinateur est connecté. Le choix du profil apparaît lors du branchement à un nouveau réseau. Le moins sécurisé est celui du « réseau domestique » qui autorise le partage de ressources (répertoires, imprimantes). Si vous n'avez qu'un seul ordinateur, le profil réseau public est adapté et vous permettra de réduire le nombre de services réseau activés. Rendez-vous dans le *Panneau de configuration > Réseau et Internet >Centre Réseau et partage* pour vérifier quel profil est actif sur votre connexion réseau. Vous pourrez en changer simplement en cliquant sur le lien au-dessous du nom de votre connexion. Ces profils correspondent aussi à l'ouverture/fermeture des ports réseau dans les règles de pare-feu. Ce dernier est accessible en tapant « pare-feu » dans le menu *Démarrer > champ de recherche*. Cliquez sur *Pare-feu Windows avec fonctions avancées de sécurité* pour le paramétrer. Le pare-feu avancé va vous permettre de créer des règles sur le trafic entrant mais aussi sur les données sortantes. Pour une configuration sécurisée, vous pouvez opter pour interdire tout trafic sortant et accorder les autorisations application par application.

La sécurité d'Internet Explorer peut être personnalisée pour empêcher les téléchargements.

L'ASTUCE

COUPEZ L'HERBE SOUS LE PIED

Lorsque l'on connecte un périphérique de stockage sous Windows 7, il affiche automatiquement une fenêtre de démarrage. Certains malwares ont mis à profit ce comportement pour se propager d'ordinateur en ordinateur. Vous pourrez configurer l'exécution des supports amovibles en vous rendant dans le *Panneau de configuration > Matériel et audio >Exécution automatique*. Dans cette fenêtre, décochez *Utiliser l'exécution automatique pour tous les médias*. Vous pourrez ensuite choisir un comportement personnalisé par type de média. Pour les logiciels/jeux et contenus mixtes, choisissez *Ne rien faire*.

Pour cela, il suffit de cliquer sur *Propriété du pare-feu* dans la fenêtre *Pare-feu Windows avec fonctions avancées de sécurité*. Repérez le profil utilisé pour votre connexion et rendez-vous dans l'onglet idoine. Ensuite, pour créer une nouvelle règle de pare-feu, revenez sur l'interface générale et faites un clic droit sur *Règle de trafic sortant* puis choisissez *Nouvelle règle*. Attention, cependant, une configuration bloquant le trafic sortant est complexe à mettre en place, car vous devrez créer des règles pour chaque application.

Smartscreen et les sécurités d'IE

La sécurité en ligne est évidemment l'affaire du navigateur. Celui de Microsoft possède notamment un filtre SmartScreen d'une efficacité redoutable contre les sites de phishing. Activé par défaut, celui-ci se manifeste dans la barre d'état au bas de la fenêtre d'Internet Explorer. Le navigateur fonctionne en mode « protégé » (quel que soit le profil utilisateur, contrairement à ce qu'il se passait sous Vista). Ce mode limite considérablement les éléments du système auxquels le navigateur a accès. Son état est indiqué au bas d'Internet Explorer. La sécurité du navigateur est accessible en cliquant sur *Outils* puis *Options internet*. Dans l'onglet *Sécurité*, vous pourrez choisir le niveau de restriction suivant si vous naviguez sur un site internet et intranet. En cliquant sur *Personnaliser*, vous pourrez choisir d'activer ou de désactiver des éléments précis. Cette liste peut interdire le téléchargement de tout fichier à partir du web. **Jean-Philippe Bay**

Pratique | Gérez les accès aux documents et répertoires

1 DONNEZ ACCÈS AUX DOCUMENTS Ouvrez l'explorateur de fichier puis rendez-vous sur le répertoire à partager avec un autre utilisateur. Faites un clic droit dessus et choisissez *Propriété pour modifier l'accès*.

2 DONNEZ ACCÈS AUX DOCUMENTS (2) Dans l'onglet *Sécurité*, cliquez sur *Modifier* puis sur *Ajouter*. Indiquez le nom de l'utilisateur et dirigez-vous sur *Vérifier les noms*. Cliquez sur *OK*, sélectionnez l'utilisateur et cochez *Contrôle total*.

3 CHANGEZ LE PROPRIÉTAIRE Dans l'onglet *Sécurité* cliquez sur *Avancé* puis, dans *Propriétaire*, sur *Modifier*. Cliquez sur *Autre utilisateur* et indiquez le nom du profil. Cochez *Remplacer* pour que tous les fichiers soient réattribués à cet utilisateur.

Release by TEAM-DZ

Astuces express

MATÉRIEL REQUIS
Matériel

NIVEAU
Facile

QUESTION

Une carte mémoire a une durée limitée et n'est pas aussi solide qu'elle peut paraître. Elle doit être manipulée avec prudence pour éviter de l'endommager. Comment prolonger sa durée de vie ?

Ménagez vos cartes mémoire

> Manipulation soigneuse Insérez ou retirez la carte avec précaution. Éteignez l'appareil photo avant d'insérer ou de retirer la carte mémoire. Ne l'enlevez pas pendant qu'une image est en cours de sauvegarde. Sur la plupart des appareils, un voyant indique que celui-ci écrit sur la carte. Tout champ magnétique externe peut endommager les cartes ou altérer les fichiers qu'elles contiennent. Ne les approchez pas des téléviseurs, des haut-parleurs, des radios … Manipulez les cartes prudemment. Tenez-les par leurs bords latéraux en évitant de toucher les contacts. Rangez-les à l'abri de la poussière, des fortes chaleurs et de l'humidité. Le plus simple consiste à les conserver dans leur petit boîtier en plastique transparent. Pour transférer les photos de la carte sur le PC, évitez de connecter l'appareil photo au PC. Passez plutôt par un lecteur de cartes connecté à l'ordinateur. Le transfert sera plus rapide et plus direct, ce qui limite les risques d'erreurs. En cas de souci ou après une utilisation intensive, formatez la carte. Insérez-la dans le lecteur de votre PC. Ouvrez l'Explorateur Windows. Cliquez du bouton droit sur l'icône de la carte et choisissez la commande *Formater*. Choisissez le format FAT32, compatible avec quasiment tous les appareils et avec toutes les versions de Windows. ■

MATÉRIEL REQUIS
Windows 7 et Vista

NIVEAU
Moyen

QUESTION

À l'installation de Windows, un compte administrateur est créé : on peut changer le nom qui lui a été attribué. Peut-on modifier aussi le nom de l'ordinateur dans le réseau, ainsi que le nom du dossier personnel ?

Changez le nom de votre ordinateur et de votre compte

> Modifiez le nom d'utilisateur Dans le Panneau de configuration, ouvrez le module *Comptes d'utilisateurs* et cliquez sur *Modifier votre nom de compte*. Entrez le nouveau nom et validez en cliquant sur *Changer le nom*. Ce nouveau nom apparaîtra dans l'écran d'ouverture de session et tout en haut du volet droit du menu *Démarrer*.

> Renommez le dossier personnel Pour modifier le nom du dossier sur le disque dur sous *C:\utilisateurs*, il faut passer par la Base de registre. Lancez regedit et sélectionnez la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current Version*. Double-cliquez sur la valeur *Registered Owner* et remplacez le nom existant par le nouveau.

> Corrigez le nom de l'ordinateur Pour changer le nom de l'ordinateur dans le réseau, ouvrez le module *Système* du Panneau de configuration et cliquez sur *Modifier les paramètres*. La fenêtre des propriétés système s'ouvre. Dans l'onglet *Nom de l'ordinateur*, cliquez sur *Modifier*. Entrez le nouveau nom et validez avec *OK*.

Release by TEAM-DZ

Contrôlez l'exécution des programmes

AppLocker

30 minutes

Débutant

AppLocker est une fonction propre à certaines versions de Windows 7 destinée à contrôler finement les programmes autorisés à s'exécuter. C'est un moyen efficace pour verrouiller le système.

AppLocker est le moyen le plus récent pour contrôler l'exécution des programmes sur Windows. Il vient après les SRP (stratégie de restriction logicielle) mais peut s'y ajouter et même s'y substituer car il est relativement simple à mettre en œuvre. Il n'est disponible que sur les versions Entreprise, Serveur 2008 R2 et Intégrale.

Les problèmes de sécurité les plus graves sont généralement dus à l'introduction et l'exécution involontaires de programmes dans le système (c'est le cas des virus, des chevaux de Troie...) ou à l'usage par un utilisateur non autorisé d'un programme dangereux (Regedit, par exemple). L'UAC, qui se limite au contrôle de l'utilisateur, n'offre pas assez de moyens de définition de droits d'accès pour faire face à toutes les situations. Au contraire, les règles construites avec AppLocker font la différence entre programmes, scripts et installateurs. Elles prennent en compte trois caractéristiques, le chemin d'accès, la signature de l'éditeur et le condensé cryptographique de l'exécutable pour autoriser ou refuser l'exécution à tel ou tel utilisateur ou groupe. Chaque règle accepte aussi des exceptions exprimées à partir des mêmes primitives.

Ceci dit, les règles n'obéissent pas à une logique booléenne. Entre les règles ou au sein d'une règle, il ne peut y avoir de composition logique de droits sur les groupes et utilisateurs. Par exemple, si une règle interdit à un groupe donné l'exécution d'un programme et qu'une autre autorise un utilisateur membre de ce groupe, cette dernière règle est sans effet. L'interdiction a toujours la priorité et l'ordre d'application des règles n'intervient pas. Pour interdire tous les membres du groupe sauf un, il faut sortir cet utilisateur de ce groupe et le joindre à un groupe autorisé. Malgré cette limitation regrettable, il est possible de faire dans la dentelle, comme on va le voir dans la suite de l'article. Attention cependant à ne pas négliger les autres aspects de la sécurité du système, comme les mises à jour, car une faille dans un programme, fut-il autorisé par AppLocker, permettrait son détournement. Le système verrouillé par AppLocker doit devenir invincible aux virus, ceux-ci ne pouvant plus évoluer.

Philippe Roure

MODE D'EMPLOI EN 8 ÉTAPES

Activez le service *Identité des applications* Allez dans le panneau de configuration > *Système et sécurité* > *Outils d'administration* > *Services*. Cliquez du bouton droit sur la ligne *Identité de l'application* puis choisissez l'item *Propriétés*. Dans la fenêtre, actionnez le bouton *Démarrer* et positionnez le menu *Type de démarrage* à *Automatique*.

Créez des règles par défaut Applocker se trouve dans le gestionnaire de stratégies de sécurité locale secpol. msc. Cliquez du bouton droit sur *Règles de l'exécutable* et choisissez dans le menu l'action *Créer les règles par défaut*. Il ne faut pas changer leur action par défaut et il n'est pas utile ici d'y ajouter des exceptions.

Release by TEAM-DZ

Logique des exceptions Les trois règles par défaut empêchent un utilisateur ordinaire de lancer un programme situé en dehors des répertoires *Windows* et *Program Files*. Si on ajoute une règle à la liste, elle aura la priorité sur les règles par défaut que ce soit pour restreindre ou élargir les droits.

Ajoutez une restriction (1) Dans le menu, cliquez du bouton droit sur *Créer une règle* pour lancer un assistant. À la première étape, indiquez que la règle est une restriction (cochez *Refuser*). Le champ *Utilisateur ou groupe* reste à *Tout le monde*. À l'étape deux, indiquez que la condition est un chemin d'accès puis que ce chemin est Windows (%WINDIR%*).

Ajoutez une restriction (2) Faites un clic droit sur *Ajouter* avec le curseur positionné à Éditeur. Avec le bouton *Parcourir un fichier de référence*, cherchez un logiciel d'origine Microsoft. Puis, ramenez le curseur vers le haut pour ne laisser que la chaîne identifiant Microsoft (O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US).

Interdiction par hachage (1) Au chapitre *Autorisation de l'assistant*, cochez *Refuser*. Puis, cliquez sur *Sélectionner* (situé à côté du champ *Utilisateur ou groupe*), et enfin sur *Avancé* et *Rechercher* dans les fenêtres successives. Le hachage d'un fichier est l'application d'une formule mathématique qui donne au fichier un chiffre le rendant unique.

Interdiction par hachage (2) Vous pouvez alors choisir un groupe ou un utilisateur enregistré dans le système, par exemple les utilisateurs du bureau à distance ou les invités. Validez les deux fenêtres. À l'étape suivante, créez une condition basée sur le hachage du fichier puis désignez-le avec le bouton *Parcourir les fichiers*.

Testez les règles avant leur application Cliquez du bouton droit sur l'icône *AppLocker* dans la console *Stratégies de sécurité locale* pour appeler ses propriétés. Là, cochez la case *Configuré* pour les règles qui nous intéressent. Le menu permet de choisir entre le test (*Auditer*) et l'application immédiate.

Release by TEAM-DZ

Un antivirus de secours : ClamAV

De nombreux malwares **gardent un temps d'avance pour déjouer la détection des antivirus.** Vous pouvez pourtant redonner l'avantage à l'antivirus et désinfecter une machine infestée lorsque vous avez négligé la protection contre les malwares.

NIVEAU

Intermédiaire

MATÉRIEL NÉCESSAIRE

- Un graveur et un CD de 700 Mo RW.
- Une connexion rapide à internet.

TEMPS DE RÉALISATION

30 minutes

Huit pour cent des utilisateurs de PC n'ont pas installé d'antivirus (chiffre Clusif). Et même dans le cas contraire, la détection n'est jamais garantie, du fait des limites intrinsèques de ces logiciels de sécurité. Les antivirus reposent presque uniquement sur le principe de reconnaissance de signatures. S'ils fonctionnaient comme de vrais IDS (détecteur d'intrusions), par l'analyse d'actions suspectes génériques, ils généreraient une avalanche de messages incompréhensibles de la plupart des utilisateurs. Or la modification minime d'un code viral suffit à changer sa signature et à le rendre invisible à de nombreux antivirus. Une fois installés, les logiciels indésirables, bots, portes dérobées, espions de claviers, se mettent à jour pour échapper aux mises à jour des antivirus. Ils utilisent souvent un rootkit qui leur apporte une protection supplémentaire, en modifiant par exemple les structures de données du système (liste des processus, des fichiers d'un répertoire...). Dans cette course, on va redonner un avantage à l'antivirus en réalisant une détection différée depuis un autre système, exécuté sur la même machine. Inutile pour ce faire de modifier le disque et libérer une partition. Avec un CD Live, le disque n'est pas modifié, sauf au moment d'effacer les programmes indésirables.

1 Commencez par graver un CD Ubuntu Le système le plus simple capable de réaliser cette opération est Ubuntu Linux. Il est gratuit et ne pose pas de problème de licence. Sur le site www.ubuntu.com, téléchargez l'image du CD Live de la dernière version. Démarrez ensuite la machine malade avec le CD gravé dans le lecteur, lequel a la priorité au démarrage dans le BIOS. Suivant la quantité de mémoire et la vitesse du processeur, montrez-vous patient. La mémoire est nécessaire en quantité, 512 Mo ou plus, parce qu'elle doit contenir les logiciels et les fichiers que vous allez ajouter sur le disque virtuel logé en mémoire. Le CD contient en effet un navigateur et des applications bureautiques mais rien pour débusquer les virus, au moins pour l'instant. Détail important, à l'amorçage du CD, choisissez la disposition du clavier et la langue employée par le système.

2 Installez ClamTK sans « rebooter » ClamAV est un logiciel antivirus en licence GPL dont il existe des versions pour Windows, MacOS et Linux. Sur Unix, c'est un programme en ligne de commande fréquemment déployé sur des serveurs de fichiers ou de courrier. ClamTK est l'interface graphique facilitant son utilisation

CRÉEZ VOTRE CD DE SECOURS

L'intérêt d'un CD live de nettoyage « bootable » sous Ubuntu, outre sa gratuité, est d'opérer à l'abri des malwares qui ont déjà endommagé votre PC sous Windows

Release by TEAM-DZ

L'ASTUCE : DÉCALEZ LES ANALYSES DE FOND

Si Clam Av est considéré comme « léger », c'est parce qu'il ne lance pas automatiquement des scans assez lourds en tâche de fond, opérations qui ralentissent les PC. Mais il ne faut pas négliger de programmer des analyses à des heures où le PC n'est pas utilisé et surtout scanner systématiquement les clés USB, voie d'entrée fréquente de programmes nuisibles. Au besoin, il existe un module d'analyse temps réel pour ClamWin, Clam Sentinel.

sur un poste de travail. Pour installer ces logiciels, on doit lancer l'installateur de programmes Synaptic, accessible à partir du menu *System > Administration*, situé tout en haut à gauche du bureau. La première chose à faire est d'ajouter un nouveau dépôt de logiciels, par le menu de *Synaptic Settings > Repository*. Dans la fenêtre, cochez la case *Universe* avant de valider ce choix. Ensuite, Rechargez la liste des programmes à partir du bouton *Recharger*, dans la barre d'outils de Synaptic. Pour trouver rapidement ClamTK dans la liste, utilisez le système de recherche intégré, d'un clic sur l'icône *Search* de la barre d'outils. Un clic droit de souris sur le nom de ClamTK fait apparaître un menu de commandes où vous choisissez *Mark for Installation*. Acceptez alors la demande de Synaptic d'installer des logiciels supplémentaires car ils sont nécessaires au fonctionnement de ClamTK. Enfin, lancez l'installation proprement dite en cliquant sur l'icône de validation dans la barre d'outils. À noter qu'il est inutile de redémarrer après l'installation de l'antivirus, contrairement à l'usage sur Windows. Cela aurait pour même effet de rétablir le système dans son état premier, puisqu'il réside entièrement dans la mémoire.

3 Mettez à jour la base de virus

L'intérêt d'une recherche de virus depuis un autre système est que le temps est à l'avantage de l'antivirus. Si le système infecté est déconnecté d'internet, le bot (virus) qu'il héberge éventuellement ne peut pas contacter son réseau (botnet) pour y télécharger ses mises à jour. Plus le temps passe, plus les contributeurs à ClamAV ont du temps pour identifier le virus et intégrer une signature correspondante dans la base. S'il est examiné au bout de plusieurs jours avec un antivirus dont la base de signature est toute fraîche, il a de très fortes chances d'être capturé. Les nouvelles menaces sont répertoriées en quelques heures. Mais si vous pouvez attendre quelques jours, c'est mieux. Pour mettre à jour la base, ouvrez un terminal (menu *Application >Accessoires*) et tapez-y *sudo su* puis *freshclam*.

4 Montez le système de fichiers FAT32/NTFS

Le système Windows se trouve sur une partition du disque. Elle est en général en FAT32 mais plus sûrement en NTFS, formats sur lesquels Ubuntu lit et écrit sans problème. Par défaut, la partition n'est pas montée, c'est-à-dire qu'elle n'est pas accessible depuis Ubuntu. Le montage s'effectue en sélectionnant la partition Windows à partir du menu *Raccourcis*. S'il existe plusieurs partitions, repérez la bonne à partir de sa taille. Une fois le système de fichiers de Windows rendu accessible, vous pouvez le parcourir avec l'explorateur de fichiers. Depuis Windows, un rootkit pouvait cacher des fichiers mais ici, ils apparaîtront à un œil expert ou à un antivirus.

5 Désinfectez et réinstallez vos logiciels

Le lanceur de ClamTK est rangé dans le menu du bureau *Applications > Accessoires*. Dans la barre de menu de l'application, choisissez *Scan > Scan Recursif* et désignez un répertoire où se trouve Windows. Au terme de l'analyse, le programme affiche les résultats. Le taux de faux positifs de ClamAV est extrêmement faible, un malware reconnu par lui est une confirmation d'infection. Pour chaque fichier suspect, les options sont de supprimer, placer en quarantaine ou ne rien faire. ClamAV n'est pas conçu pour réparer les dégâts causés par un programme viral. La façon la plus sûre de restaurer le système et les logiciels est de les réinstaller à partir du média d'origine. Ici, il est préférable de supprimer ou désactiver tous les programmes nuisibles signalés comme tels.

6 Installez un antivirus sous Windows

Une fois Windows sur pied, il faut lui donner un antivirus. Même si aucun n'est infaillible, il en existe de très bons, gratuits et légers. C'est le cas de ClamAV pour Windows, qui s'appelle ClamWin (www.clamwin.org). Contrairement à la plupart des antivirus, il ne scanne pas les fichiers à l'ouverture et à la copie. Ainsi, il n'interfère pas du tout avec les opérations du système (copie, ouverture de fichiers...). **Philippe Roure**

Release by TEAM-DZ

Sauvegardez sur mesure avec BackItUp 10

On ne cessera de le répéter, **la sauvegarde de données permet de se prémunir de tout dysfonctionnement hardware ainsi que des erreurs de manipulation.** Nero propose une solution très simple, que le matériel soit fixe ou nomade !

NIVEAU

Intermédiaire

MATÉRIEL NÉCESSAIRE

- **Lecteur-graveur CD/DVD**
- **Nero BackItUp 10 (www.nero.com/fra/backitup-and-burn-overview.html)**

TEMPS DE RÉALISATION

15 à 30 min

Intégré dans la suite Nero 10 Platinum HD, BackItUp & Burn propose la sauvegarde/récupération de dossiers, fichiers et même du système complet. Plusieurs méthodes de sauvegarde sont disponibles. La plus simple assure une sauvegarde complète, incluant toutes les données des supports de stockage connectés ainsi que des périphériques (clé USB, par exemple). Cette méthode est utile pour la première opération, afin de créer une base de données intégrale. La sauvegarde de plusieurs systèmes complets peut s'avérer utile, notamment en cas de changement de PC, revente, prêt, etc. Autre intérêt évident : certains logiciels anciens - mais encore utilisés quotidiennement - ne fonctionnent pas forcément sous un OS récent comme Windows 7. Par ailleurs, il convient aussi de paramétrer les sauvegardes, qu'elles soient automatiques (il faut alors en fixer la fréquence) ou manuelles. Enfin, et c'est sans doute le choix le plus délicat, il faut définir le protocole de sauvegarde. Le mode « incrémentiel » écrase les sauvegardes précédentes en remplaçant toutes les données antérieures (seule la chronologie importe), tandis que le mode « différentiel », plus rapide, assure uniquement la sauvegarde des données nouvelles, conservant intégralement les précédentes.

1 Configurez une sauvegarde sélective

Choisissez l'onglet *Sauvegarder* (en haut à gauche) pour atteindre la Sauvegarde de fichiers. Dans la zone de travail s'ouvre alors un explorateur où vous sélectionnez les dossiers à sauvegarder. Attention : il est indispensable de cocher ces dossiers dans le volet gauche pour pouvoir sélectionner tout ou partie de leur contenu dans le volet droit. Confirmez par un double-clic puis validez en vous dirigeant sur la flèche verte en bas à droite. À ce stade, BackItUp considère que les « sources » sont définies. Vous pouvez d'ores et déjà modifier la période d'exécution de la tâche en cours, en cliquant sur une date choisie dans le calendrier inférieur gauche. Le logiciel permet à tout instant ce type de planification et même d'enregistrer les modifications en cours.

2 Définissez précisément le dossier cible

Le menu *Présentation générale* (supérieur gauche) confirme l'étape de sélection des cibles. Vous pouvez choisir tous les *Disques durs* connectés, le *Disque optique*, les *Périphériques amovibles*, le *Réseau* ou le *Stockage en ligne*, puisque BackItUp assure le chargement distant sur un espace dédié Nero ou un FTP. Nous

LE CHOIX DE LA SIMPLICITÉ

Nero BackItUp se distingue de ses concurrents par son interface intuitive et sa simplicité d'utilisation. Ses options avancées intéresseront également les utilisateurs expérimentés.

1

2

Release by TEAM-DZ

L'ASTUCE : L'ANTICAUCHEMAR

On peut vouloir procéder à une sauvegarde complète et rapide sans désirer se soucier des paramétrages complexes du logiciel. Grâce à la touche *Autobackup*, le logiciel prend en charge tous les réglages du PC. Cet outil est accessible depuis le menu *Sauvegarder > Sauvegarde automatique > 1er choix*. Il suffit de définir une fois pour toutes la cible (*Disque dur* par exemple) pour activer Autobackup. Les fois suivantes, un clic suffira pour lancer l'opération…

avons opté ici pour le disque dur (D:) Data. Pour définir le chemin d'accès (champ éponyme) cliquez sur le bouton *Parcourir* et spécifiez un nom de dossier. Plusieurs cibles peuvent être définies simultanément: en cliquant sur *Périphériques amovibles*, le logiciel invite à enregistrer le protocole de la première opération avant d'en définir le second (sur clé USB ou autre). En gravure, il faut en revanche attendre la fin de l'opération.

3 Sauvegardez facilement sur plusieurs cibles !

Gain de temps évident à la clé, BackItUp autorise les sauvegardes simultanées. Le nombre de cibles, illimité, s'affiche dans le volet de travail central, sous forme de bandeau de sélection (cinq icônes). Après en avoir défini une première comme dans l'étape précédente, cliquez sur le bouton *Ajouter la cible* en bas à droite de l'interface principale pour qu'un second bandeau de sélection s'ouvre et ainsi de suite pour le troisième… La limite de l'exercice, rappelons-le, est de lancer une sauvegarde par gravure sur disque optique, toujours plus longue (même à vitesse maximale) que sur l'un des disques durs connectés ou l'un des Périphériques amovibles en USB 2. Des sauvegardes sur plusieurs graveurs CD sont possibles, mais alors gérées par Nero Burning Rom.

4 Prenez le temps de peaufiner la finalisation !

Après validation (flèche verte inférieure droite), la *Présentation générale* confirme l'opération *Finaliser*. Le volet central se garnit alors de menus déroulants permettant au choix de finaliser par sauvegarde complète, incrémentielle ou différentielle; le cas échéant, vous pouvez y ajouter des commentaires (bouton éponyme). Le bandeau *Options* s'avère très utile: vous y définissez la compression (faible, normale, élevée), le cryptage (aucun, classique ou AES) et, en cas de cryptage activé, l'assignation d'un mot de passe, assorti d'un indice de rappel. La sécurisation des données confidentielles ou sensibles est donc très simple, mais se limite au mode manuel, sauf si vous voulez répéter des sauvegardes sécurisées successives (mode sauvegarde automatique permis).

5 Surveillez le processus final !

Quel que soit le type de sauvegarde choisi, BackItUp en indique l'état d'avancement. Après avoir validé le processus dans la fenêtre centrale, vous pouvez toujours revenir en arrière en cas d'oubli ou d'erreur, ou bien procéder à son lancement. Le menu gauche *Présentation de la tâche* est prêt pour l'affichage de la progression. Attention ! Par défaut, sous Vista ou Windows 7, une confirmation de l'OS est systématiquement demandée. Veillez donc, notamment s'il s'agit d'une sauvegarde volumineuse, à autoriser son lancement. Durant la création de la ou des sauvegardes, l'avancement en pourcentage (Cf. capture 5) s'affiche sous la *Présentation de la tâche* (barre graphe vert) jusqu'à son terme: le statut final coché *OK* s'affiche alors. L'archive créée apparaît après un double-clic sur le nom de la sauvegarde datée.

6 Une sauvegarde de masse pour terminer !

À la maison comme au bureau, la sécurité n'est pas un luxe: sauvegarder une ou plusieurs unités complètes garantit la tranquillité d'esprit. BackItUp se charge de ces tâches en procédant toujours par la même méthode: identification et sélection des « sources », choix des cibles et finalisation.
Dans le menu *Sauvegarder*, optez pour le troisième choix, *Sauvegarde d'unité*. Le volet central dévoile alors automatiquement tous les supports de stockage connectés, partitions comprises. Il ne vous reste plus qu'à cocher le ou les volumes désirés, valider la sauvegarde (flèche verte inférieure) et définir le disque de destination. Cette tâche peut être automatisée depuis le volet de programmation, à la ligne *Modification et Gestion des tâches*.

Jean-Pierre Carles

Release by TEAM-DZ

Sauvegardez plus rapidement avec Rebit

La perte de données reste l'un des problèmes permanents de l'informatique. **Réaliser des sauvegardes quotidiennes s'avère incontournable mais comment suivre l'évolution de votre système ?**

NIVEAU

Débutant

MATÉRIEL NÉCESSAIRE

- PC doté d'un lecteur de CD
- Windows 7, Vista ou XP
- Rebit SaveMe Express

TEMPS DE RÉALISATION

40 minutes

Les systèmes de sauvegarde présentent presque tous au moins deux défauts : la sauvegarde du système entier est rarement complètement effectuée et les fichiers ne sont enregistrés qu'à des intervalles plus ou moins éloignés. Lorsqu'il s'agit de restaurer ce que l'on croit avoir sauvegardé, la réalité est parfois très décevante. Comment récupérer un fichier modifié à maintes reprises ou redémarrer un ordinateur dont le système ne donne plus signe de vie ? Le logiciel Rebit SaveMe Express prétend résoudre ces problèmes avec, en particulier, la restauration via le CD de boot inclus. Attention cependant, ce logiciel nécessite un disque dur dédié à son fonctionnement. Comme l'application peut gérer l'USB, vous pouvez investir dans une unité de sauvegarde portable. Cependant, un disque dur interne vous apportera plus de rapidité lors d'une restauration et ne ralentira pas votre système. Côté taille, Rebit sait gérer l'espace disque en effaçant automatiquement les anciens fichiers dès lors qu'il a effectué un point de restauration du système. Ainsi, la taille de la sauvegarde ne devrait pas atteindre des sommets par rapport aux données originales qui sont sur votre disque dur.

1 Mettez le logiciel en place Rebit SaveMe Express enregistre le moindre changement sur l'un de vos fichiers et permet de revenir sur n'importe quelle version de ce dernier. Il permet aussi de restaurer entièrement votre système grâce à un CD de démarrage. Ainsi, vous pourrez revenir sur n'importe quelle configuration de votre système. Le logiciel est téléchargeable en version d'essai limitée à trente jours à cette adresse : www.microapp.com/logiciel_rebit_1452.html (29,95 €). Lors de l'installation, choisissez l'emplacement qui servira à stocker les données. S'il n'est pas aussi important que le disque à sauver, il n'apparaîtra pas. Ensuite, laissez le logiciel effectuer la sauvegarde. Pour savoir où il en est, cliquez sur l'icône dans la zone de notification.

ASTUCE : WINDOWS 7 POURRAIT LE FAIRE

Windows 7 peut aussi enregistrer à intervalles réguliers toutes vos données. Caché dans le menu *Démarrer > Tous les programmes > Maintenance*, l'outil *Sauvegarder et restaurer* requiert un second disque dur. En vous rendant dans l'« outil de planification » de Windows 7, vous pourrez créer une tâche pour réveiller l'ordinateur et effectuer des opérations planifiées. La sauvegarde est enregistrée dans le répertoire *Microsoft > Windows > Windows Backup* et se nomme « automatic backup ». Éditez cette tâche puis cliquez dans le planificateur pour sortir du mode veille et l'exécuter.

Release by TEAM-DZ

LA SAUVEGARDE DE WINDOWS
Windows 7 propose un outil de sauvegarde intégré. Certes, il n'a pas les qualités de Rebit mais il peut être très utile pour restaurer un PC. Rendez-vous dans le menu *Démarrer > tous les programmes > maintenance*. Une fois le programme lancé, diquez sur *Configurer la sauvegarde*. Choisissez ensuite votre unité de sauvegarde. L'application vous propose de gérer elle-même les fichiers qui seront sauvegardés. La sauvegarde par défaut inclut les programmes Windows ainsi que les fichiers contenus dans les répertoires de tous les utilisateurs (documents, favoris, fichiers Outlook…) . Si vous stockez vos documents dans des répertoires différents, optez pour l'option *Me laisser choisir*. Sélectionnez alors les éléments à ajouter en cochant les cases devant les dossiers/ fichiers. Dans la page suivante, cliquez sur *Modifier la planification*. N'oubliez pas que votre ordinateur doit être allumé pour dédencher la sauvegarde. Une fois la sauvegarde effectuée, vous pourrez choisir la date de votre restauration et les fichiers à restaurer. Si votre système ne fonctionne plus, le DVD de Windows 7 vous proposera d'utiliser ces sauvegardes pour restaurer Windows et vos données.

2 Découvrez l'interface du programme

L'opération de sauvegarde et de catalogage peut prendre pour la première fois plusieurs heures. Durant cette opération, pas moins de quatre processus, visibles dans le gestionnaire de tâches, opèrent. Il faut être patient et attendre que l'opération arrive à son terme. Une fois la sauvegarde terminée, ouvrez l'explorateur de fichier (touches [Windows] + [E]). Cliquez sur l'unité de sauvegarde Rebit. L'ensemble de l'arborescence de votre disque s'y trouve reproduit. Les documents de chaque utilisateur sont directement accessibles dans des répertoires virtuels. Précisons que Rebit SaveMe nécessite l'utilisation d'un volume disque au minimum de la même taille que celui qu'il surveille. Lui-même pour son propre fonctionnement exploite 300 Mo. Un espace de stockage largement plus grand que l'original vous sera utile avec le temps et les successives sauvegardes. Nous vous conseillons de dédier un disque dur complet à cette tâche pour ne pas surcharger le disque système en opérations d'écriture et en données.

3 Récupérez une version d'un fichier

Pour trouver l'une des versions d'un fichier, rendez-vous dans le disque de sauvegarde puis cliquez sur le document. Toutes les versions enregistrées par Rebit s'afficheront alors. Vous pourrez récupérer le document en le rapatriant à l'aide de la souris dans l'espace de départ. Le logiciel fonctionne sous XP, Vista et Windows 7 en version 32 ou 64 bits. Il inclut dans sa version la plus récente une fonction originale appelée Smartsave, qui vous permet d'ajuster le nombre de fichiers à « backuper » pour les remplacer par un autre contenu plus intéressant. L'opération s'effectue dynamiquement, mais il faut un autre support, comme une clé USB ou un CD-ROM, pour éviter de saturer un disque

4 Récupérez votre système avec le CD

Cette procédure vous permet de récupérer un état viable mais ancien de tout votre système. Cela peut vous permettre d'effacer un virus et de retrouver un environnement stable. Lancez votre ordinateur sur le CD fourni avec Rebit ou téléchargez l'image à l'adresse www.rebit.com/support.html. Une fois que vous aurez paramétré la langue d'affichage, choisissez la partition utilisée par Rebit. Cochez l'emplacement de votre disque système et la date à laquelle vous voulez le restaurer. Attribuez le disque et la sauvegarde qui va avec en les sélectionnant et en cliquant sur *Attribuer*. Lancez la restauration. Celle-ci peut prendre un certain temps.

5 Planifiez précisément la restauration

Ne planifiez pas la restauration de vos données à un horaire trop proche des dernières opérations ou transferts, surtout si ceux-ci dépendent des encombrements du réseau. Les données écrites sur le même disque après l'heure du début de la restauration seront effacées, ce qui risque de créer des incohérences, en particulier dans le cas de bases de données où les index sont justement mis à jour à la fin des opérations. Le problème se pose en restauration sur un disque particulier mais pas en sauvegarde, car Rebit protège « son disque » en écriture afin d'éviter l'intervention d'autres logiciels. **Jean-Philippe Bay**

Release by TEAM-DZ

Restaurez des données effacées

Recuva 1.39.509

60 minutes

Difficulté

Effacer un fichier par maladresse ou inadvertance est si vite arrivé. Il existe heureusement des applications comme Recuva pour vous permettre de récupérer tout ou partie du contenu supprimé.

Il vous est déjà sûrement arrivé de mettre à la corbeille un répertoire qui ne devait pas l'être. Et comme un malheur n'arrive jamais seul, vous avez fini par vider la poubelle de Windows avant de vous rendre compte de votre erreur. Ce stéréotype colle parfaitement aux problématiques liées aux solutions de restauration de fichiers. Recuva fait partie de ces programmes dédiés à cet usage. Cette application open source dite de la « dernière chance » a pour mission d'analyser les volumes (interne et externe) de l'ordinateur afin de traquer le moindre fichier récupérable. On peut même augmenter ses chances en choisissant le ou les emplacements cibles à fouiller. Recuva se distingue de la concurrence par une compatibilité sans égale. Il gère en standard de nombreux supports : les disques durs, les médias amovibles (carte mémoire, clé USB, etc.) et même les baladeurs iPod. Une fois la recherche terminée, l'application vous permet dans la mesure du possible de restaurer les fichiers retrouvés. Son système de classement intuitif, basé sur le principe d'un feu tricolore, vous permet de connaître instantanément les chances de réussite du processus de restauration.

Cet utilitaire est sans doute l'un des plus efficace de ce domaine si particulier. Cela ne veut pas dire qu'il est pour autant parfait. Il n'existe pour l'heure aucune solution logicielle capable d'atteindre un taux de réussite proche des 100 %. La raison est simple : cela dépend bien souvent de la configuration sur laquelle l'application est déployée, du type de média et de la méthode de suppression utilisée. Seules des sociétés spécialisées dans le domaine, comme Chronodisk ou Kroll Ontrack, peuvent vous garantir un taux de réussite plus élevé. Il vous faudra toutefois débourser plusieurs centaines voire milliers d'euros en fonction du volume à restaurer. Les photos de vos dernières vacances méritent-elles un tel investissement ? Recuva peut dans certains cas suffire à satisfaire vos besoins. Sur ce marché de la restauration de fichiers, on peut aussi citer File Scavenger V3.3, Restoration 2.5, FreeUndelete, UndeletePlus , Recover My Files et Disc Data Recovery de Disk Doctors. Cette dernière firme propose d'ailleurs différentes versions pour restaurer les fichiers d'applications bien spécifiques. ■

MODE D'EMPLOI EN 6 ÉTAPES

Démarrez une recherche L'application est dotée d'un assistant qui se lance au démarrage. Il guide les débutants dans le processus de recherche des fichiers effacés. Les avertis peuvent s'en passer en cliquant sur l'option *Annuler*. Ils auront alors la possibilité de définir tous les paramètres pour affiner leur recherche de documents.

Choisissez le type de documents à retrouver Recuva vous permet de récupérer tous les types de fichiers (photos, vidéos, texte, musique, etc.). Cochez pour cela la case qui correspond à vos besoins puis cliquez sur *Suivant*. Attention, vous ne pouvez faire qu'un seul choix à la fois.

Release by TEAM-DZ

Où doit-il chercher ? Cette étape vous donne le choix entre quatre emplacements prédéfinis (Corbeille, Mes documents, emplacement spécifique, etc.). Il existe toutefois une option baptisée *Je ne suis pas sûr*, qui propose un scanne complet de tous les emplacements internes ou externes de l'ordinateur.

Augmentez vos chances Une fois le questionnaire permettant à l'assistant d'optimiser ses recherches terminé, Recuva va pouvoir procéder à la recherche des fichiers perdus ou effacés. N'hésitez pas à cocher l'option *Activer l'analyse approfondie*. Cela a pour effet de ralentir le processus mais c'est aussi plus efficace.

Processus de recherche Le temps dévolu à l'analyse des emplacements définis dépend bien entendu des paramètres définis mais aussi et surtout de leurs capacités. Comptez environ une trentaine de minutes pour un disque dur de 250 Go avec l'option *Autre fichier* sélectionnée à l'étape 2.

Restauration des fichiers Recuva liste enfin l'ensemble des fichiers récemment supprimés. L'application utilise un code couleur (rouge, orange, vert) informant l'utilisateur sur sa capacité ou non à récupérer le document en question. Cochez les documents que vous souhaitez restaurer et cliquez sur *Récupérer* en bas à droite.

UNE SOLUTION INTUITIVE ET VISUELLE

Le mode avancé vous permet d'aller plus loin avec Recuva. L'utilisateur peut par exemple avoir plus de détails sur les fichiers qui ont été retrouvés lors de l'analyse. L'application fait en premier lieu un classement par date de dernière modification. Recuva utilise aussi et surtout un code couleur basé sur le principe des feux tricolores (rouge, orange, vert). Ce premier niveau d'information permet à l'utilisateur de connaître l'état du document. Le rouge étant bien entendu associé à un statut d'irrécupérable, l'orange donnant des chances très faibles à l'inverse du vert qui est excellent. Recuva offre également dans certains cas un aperçu du document à restaurer. Les utilisateurs experts ont même accès à l'en-tête du fichier. Une information qui demande des connaissances approfondies, ce n'est donc pas à la portée de tous.

Dans l'analyse approfondie, sous l'onglet *Type de vue*, il est possible de choisir le mode d'affichage des fichiers récupérés. On les retrouvera sous forme de listes, d'arborescence, pour visualiser leurs emplacements, et de vignettes pour faire apparaître les fichiers supprimés sous forme de graphiques ou d'images. Lors de la récupération, il arrive parfois qu'un fichier signalé en couleur orange ne soit finalement pas récupérable. Il se peut que certains fichiers soient beaucoup trop endommagés, voire tout simplement irrécupérables. Recuva n'a pas forcément la solution dans ce cas-là. C'est tout de même une des applications les plus efficaces dans ce domaine.

Release by TEAM-DZ

Échappez au crash du système d'exploitation

Norton Ghost 14

60 minutes

Difficulté

Un crash de l'OS peut prendre en otage des fichiers de grande valeur. Voilà pourquoi une solution de création d'image disque et de sauvegarde automatisée peut sauver de nombreuses heures de travail.

MODE D'EMPLOI EN 8 ÉTAPES

Installez Norton Ghost Rendez-vous dans la boutique en ligne de Norton (www.buy.norton.com) pour y acheter et télécharger la version française de Ghost 14, version strictement identique à la version boîte vendue dans les rayonnages. Les formalités d'achat passées, procédez à l'installation de Ghost .

Mise à jour par le LiveUpdate L'installation terminée, l'application vous invitera à redémarrer le PC. Faites-le puis double-cliquez sur l'icône de Ghost et entrez-y le numéro de série vous ayant été fourni à l'achat. Nous vous recommandons ensuite d'exécuter le LiveUpdate pour mettre Ghost à jour.

La planification des processus Au premier démarrage, l'utilisateur peut planifier des processus à l'aide d'un assistant. Dans la colonne de gauche cliquez sur *Tâches* puis sur *Exécuter ou gérer les sauvegardes* dans la zone centrale pour atteindre le module de planification.

Programmez les jours et les horaires Par défaut, le logiciel est programmé pour déclencher une sauvegarde tous les dimanches et jeudis, mais une fois par semaine suffit. Ces sauvegardes ne tiennent compte que des modifications opérées depuis la dernière image, ce qui permet d'économiser de l'espace disque.

Release by TEAM-DZ

5

Utilisez les déclencheurs d'événements L'application peut être programmée pour générer une sauvegarde de vos fichiers en fonction de certaines actions, comme l'installation d'un nouveau programme. Cliquez sur *Général* sous l'intitulé *Déclencheurs d'événement* pour atteindre les déclencheurs d'événement.

6

Fichiers à sauvegarder Ghost est configuré par défaut pour effectuer des sauvegardes incrémentales des dossiers Windows : *Mes Documents*, *Mes Vidéos*, *Mes Images* et *Mes Musiques* ainsi que les favoris Internet Explorer et les paramètres du bureau. Ajoutez des dossiers et différents types de fichiers en cochant les cases idoines.

7

Destination de l'image disque et des sauvegardes Cette étape se limite simplement au choix du média cible qui accueillera non seulement l'image mais aussi les sauvegardes programmées. Norton Ghost tente de choisir une destination appropriée, comme un disque dur externe par exemple.

8

Débutez la sauvegarde Une fois que tout est défini, cliquez sur le bouton *OK*, sélectionnez la fonction *Effectuer ma première sauvegarde* puis pressez *OK* à nouveau. Norton Ghost va alors débuter la création de l'image disque à laquelle viendront s'ajouter les sauvegardes incrémentales ultérieures.

RETROUVEZ UN SYSTÈME SAIN

Il arrive que votre OS ne soit plus sain ou fonctionnel. La seule solution est dans ce cas précis la restauration d'une image disque préalablement créée avec Ghost. Il faut pour cela vous munir du CD de démarrage, fourni dans la boîte ou téléchargé lors de l'achat en ligne, et du disque dur externe où sont stockées l'image et les sauvegardes. Insérez le CD dans le lecteur optique de l'ordinateur et bootez dessus. Dans l'interface qui s'affiche, cliquez sur l'onglet *Restauration* et choisissez la fonction *Récupérer mon ordinateur*. C'est à ce moment précis que vous choisissez l'emplacement de votre sauvegarde initiale. L'installation peut prendre une bonne demi-heure selon la taille du disque à restaurer. Une fois le processus terminé, redémarrez l'ordinateur pour retrouver Windows. Il se peut que la dernière image disque ne contienne pas les dernières sauvegardes. L'utilisateur doit donc restaurer de manière individuelle des fichiers. Cliquez sur *Récupérez des fichiers* depuis l'écran d'accueil de Ghost.

Release by TEAM-DZ

Diagnostiquez votre ordinateur

Aida64 Extreme Edition

10 minutes Initié

Que ce soit pour mettre à jour votre configuration ou en vue de déceler des dysfonctionnements, les logiciels de diagnostic et d'évaluation permettent d'examiner les composants de votre PC.

Pour illustrer ce pratique, nous avons installé le logiciel Aida64 Extreme Edition en version 1.6 Bêta. Anciennement Everest Ultimate Edition, ce logiciel complet est doté d'un ensemble de fonctions de détection et d'évaluation du matériel et des systèmes d'exploitation installés sur votre ordinateur. Le processeur, la carte mère et son contenu ainsi que les périphériques branchés aux différents connecteurs sont tous auscultés et répertoriés. En plus d'identifier avec précision les composants, Aida64 Extreme Edition récolte quelques informations complémentaires selon les cas, comme les versions de pilotes et les possibilités de réglage pour améliorer les performances. Il vous relie, directement à partir de l'interface, aux sites de certains constructeurs pour télécharger les pilotes ou afficher des informations sur les composants. Enfin, il est à même d'identifier les connexions réseau et d'afficher certaines informations capitales sur les disques en partage par exemple. Enfin, Aida64 comporte un module de mesure des performances dédié aux composants les plus importants : CPU, mémoire, affichage… Ces outils de tests synthétiques permettent de situer le gain ou la perte de performances après une mise à jour par exemple.

Nous avons installé Aida64 Extreme Edition sur un PC sous Windows 7, une configuration représentative du contenu d'un ordinateur assez basique, c'est-à-dire sans autre carte additionnelle que la carte graphique, et sans la mise en œuvre de technologies complexes comme le Raid ou la virtualisation. Ceci pour montrer la relative complexité de l'exploration des entrailles d'un ordinateur, fut-il basique. Aida64 Extreme Edition est un outil de diagnostic richement doté en fonctions. Il est proposé en version d'essai, valable trente jours et limitée fonctionnellement, et en versions Extreme et Business destinées aux entreprises. Cette dernière comporte des fonctions appropriées en milieu professionnel, comme la surveillance des postes à distance. Détection, évaluation et surveillance forment le triptyque d'Aida64. Un logiciel qui devrait faire partie de la trousse d'urgence de votre informatique. ■

MODE D'EMPLOI EN 8 ÉTAPES

Une interface rappelant l'Explorateur La fenêtre d'accueil d'Aida64 affiche les différentes rubriques sur la gauche et les icônes des fonctions, ou les informations recueillies, à droite. Cliquez sur *Ordinateur* puis sur *Résumé* pour accéder à la liste des composants détectés par le logiciel et dont certains sont affichés en bleu.

Réglez les paramètres Avant de vous lancer dans la manipulation des fonctions d'Aida64 Extreme Edition, vous devrez peut-être régler quelques paramètres afin de personnaliser le logiciel selon vos besoins. Vérifiez par exemple le dossier d'enregistrement des rapports et modifiez-le si nécessaire.

Release by TEAM-DZ

Le système en un coup d'œil Cette fenêtre est le véritable centre de commande du logiciel. Elle donne le résumé du système en affichant la liste de tous les composants, logiciels et périphériques détectés. Vous devez cliquer sur le bouton gauche pour accéder aux fonctions spécifiques.

Des liens actifs Les composants affichés en bleu sont accessibles comme des liens, ce qui vous permet d'effectuer quelques opérations supplémentaires. Cliquez avec le bouton gauche de la souris sur l'un des composants en bleu, un menu s'affiche et vous propose des informations sur le produit sélectionné ou la mise à jour du pilote.

Sondez la température Dans le menu à gauche, cliquez sur *Sonde* pour afficher les températures et les voltages de vos composants principaux : GPU, CPU et carte mère. Cette fonction peut être un point de départ pour détecter d'éventuelles surchauffes, par exemple si vos ventilateurs tournent en permanence au maximum.

Auscultez les composants Les options proposées dans cette fenêtre permettent de récolter les références exactes des composants les plus importants intégrés à la carte mère : CPU, Mémoire, Bios, chipset… Dans la section *Carte mère* vous pouvez accéder aux liens vers les sites des fabricants du BIOS et la carte mère.

Vérifiez les processus actifs Les informations livrées sur l'OS ne se limitent pas à la version détectée, mais sont une véritable mine de renseignements sur ce qui s'y passe. Cliquez sur *Processus* pour afficher la liste des exécutables actifs et des processus du système. Un double-clic sur un processus affiche la fenêtre des propriétés de l'exécutable.

Testez vos composants Cliquez sur l'option *Performances* en bas de la liste de gauche pour accéder aux tests de performances des composants. Cliquez sur un type de test puis sur *Rafraîchir* pour lancer le test. Cette fonction peut être utilisée pour vérifier le gain, ou la perte, de performances après une mise à jour par exemple.

Release by TEAM-DZ

Retrouvez vos fichiers disparus

Trop tard, vous avez effacé par erreur vos précieux documents ou sublimes photos de vacances. Arrêtez de pester contre cette « satanée machine de malheur ». Respirez : **tout n'est pas perdu.** Il y a même de fortes chances de tout récupérer. Suivez le guide…

NIVEAU

Confirmé

MATÉRIEL NÉCESSAIRE

- PC
- Disque dur

TEMPS DE RÉALISATION

30 minutes

L'erreur est humaine, la réparation est technique. Professionnel ou simple débutant, la suppression accidentelle de données est loin d'être un incident isolé… L'augmentation massive des données cheminant dans le disque dur, via des cartes mémoire, dés USB ou même internet engorge toujours plus vite nos espaces de stockage. Pour grappiller quelques mégaoctets ou juste faire le ménage sur son PC, on efface des dizaines de fichiers pour s'apercevoir, trop tard, qu'ils étaient importants. Heureusement, on a l'habitude de faire un simple [Suppr] ou clic droit Supprimer, pour effacer un fichier. Cette opération a pour conséquence de transférer le fichier effacé dans la Corbeille. Mais il n'a pas disparu du disque dur, et un clic droit sur le fichier puis Restaurer permet de l'enlever de la Corbeille. En revanche, si vous videz celle-ci ou appuyez sur [Maj] pendant que vous enfoncez la touche [Suppr], le fichier sera « définitivement supprimé » selon l'expression de Windows. En réalité, il est simplement enlevé de l'arborescence de fichiers pour l'OS. L'espace sur le disque dur est donc libéré, mais les clusters (plus petites zones de stockage d'un disque dur) ne sont pas touchés.

Limitez les dégâts lors de l'effacement

Toutefois, dès que le système d'exploitation a besoin de place pour stocker des données, il écrasera tôt ou tard les octets contenus sur les clusters du fichier supprimé. La création d'un fichier temporaire, la copie d'un fichier ou toute autre opération pourrait bien anéantir vos chances de retrouver votre fichier effacé. Aussi, plusieurs précautions sont à prendre avant toute tentative de récupération. Ne déplacez pas des fichiers ou dossiers qui menaceraient d'exploiter les clusters anciennement alloués à votre fichier supprimé. N'installez pas de logiciel sur la partition contenant le fichier effacé. Par ailleurs, la défragmentation va déplacer les clusters libres et occupés, réduisant ainsi vos chances de récupération. Il ne faut donc pas y recourir a posteriori. En revanche, si une défragmentation a eu lieu peu avant l'incident, non seulement elle maximisera vos chances de réussite mais le processus sera plus rapide. Dans cette perspective, nous vous invitons à utiliser un logiciel de récupération en version portable (s'exécutant sans nécessiter d'installation) ou à l'installer sur une partition différente du fichier supprimé (une clé USB, par

Pratique | Retrouvez des fichiers supprimés

> PRÉPARATION Lancez *File Recovery* et cliquez sur le drapeau pour changer la langue anglaise en français. Sélectionnez la partition de votre choix et tapez *. suivi de l'extension recherchée, ici « jpg » pour des images JPEG. Appuyez sur le bouton *Rechercher*.

> RECHERCHE Patientez plusieurs minutes, le temps que l'application débusque tous les fichiers. Une fois la recherche terminée, sélectionnez les fichiers à restaurer en appuyant sur chacun d'eux avec la touche [Ctrl] enfoncée ou à l'aide de la souris.

> RESTAURATION Cliquez sur le bouton *Restaurer* et choisissez *Restaurer* ou *Restaurer avec structure* selon que vous souhaitez les restaurer avec l'arborescence des répertoires ou non. Cliquez ensuite sur le dossier dans lequel ils seront récupérés.

Release by TEAM-DZ

Recherche Sélectionnez cet onglet pour rechercher un fichier spécifique, dont vous connaissez une partie ou la totalité du nom. Il est également possible de taper un mot contenu dans le fichier à rechercher.

Options Configurez la finesse de recherches ainsi que les différents réglages (sauvegardes, lancement…).

Sauvegardez Conservez les fichiers reconnus et sélectionnés sur CD/DVD ou autre support…

Liste des fichiers Les fichiers reconnus sont répertoriés ici. Après formatage, leur nom est éliminé, d'où les noms fantaisistes commençant par « LostFile_ ».

Fichiers retrouvés Dans ce panneau, vous visualiserez en temps réel la reconnaissance des fichiers, organisés par dossier, type de fichiers ou date.

Propriété Le fichier sélectionné est visualisé ainsi que ses propriétés, comme la fonction *Propriétés* de Windows.

Prévisualisation de fichiers Que ce soit des images, des documents bureautiques, vous pouvez généralement consulter chacun des fichiers reconnus, avant la fin de la recherche complète.

exemple). Ne tardez pas non plus avant d'essayer de récupérer vos données. Certains logiciels fonctionnent plutôt bien sur disque dur, mais refusent de récupérer les fichiers depuis les cartes mémoire ou clés USB. D'autres enfin se contentent de débusquer les fichiers perdus sur des partitions FAT et FAT 32, mais pas NTFS. Or, le système de fichiers utilisé par Windows NT, 2000, Vista ou 7 est en NTFS par défaut. C'est pourquoi nous avons réduit notre sélection au logiciel file Recovery de SoftPerfect (www.softperfect.com/), qui non seulement est gratuit et localisé en français, mais suffisamment rapide, pour peu que vous sachiez quel type de fichiers vous recherchez.

Récupérez des fichiers après formatage

Le logiciel Recover My files de GetData (www.recovermyfiles.com/fr/) autorise non seulement de restaurer des fichiers effacés, mais également de récupérer les données après un formatage accidentel ou la réinstallation ou restauration du système d'exploitation. Étant donné les services quasi prodigieux qu'il accomplit, il faudra se délester de 70 euros pour en profiter totalement. La version de démonstration n'autorise que la visualisation des fichiers potentiellement récupérables. Au lancement de l'application, vous choisirez l'option *Recover Files* si vous avez perdu ou effacé des données, si vous videz la Corbeille ou même si vous avez été victime d'un cheval de Troie ou d'un virus. Si le problème est plus sérieux (formatage accidentel avec Fdisk ou un logiciel similaire, réinstallation de Windows, restauration du système, lecteurs corrompus ou manquant), il vous faudra alors opter pour Recover a Drive. Si nous avons retenu ce cas, l'interface utilisateur et les étapes sont les mêmes dans toutes les circonstances. Commencez par sélectionner le disque physique (disque dur, clé USB…) ou logique (partition de ces derniers) en cliquant sur celui-ci. Si votre espace de stockage n'apparaît pas, vérifiez son branchement. Déconnectez et reconnectez-vous sur un autre port USB par exemple, puis cliquez sur *Refresh*. Dirigez-vous ensuite sur le bouton *Next*. Si vous savez exactement quel type de fichiers vous manque (exécutables, photos, vidéos, e-mails…), cliquez sur *Drive recovery using selected file type*, sinon cochez l'option *Automatic Drive Recovery*. Recover My files examine chaque cluster et rétablit l'arborescence des répertoires. Sans attendre que la recherche soit achevée, vous voyez en temps réel, dans le panneau de gauche, les types de fichiers reconnus et récupérables. En cliquant sur chaque dossier, puis sur un fichier vous pourrez éventuellement prévisualiser le fichier récupéré, que ce soit une image ou un document bureautique. Quand la recherche est terminée, vous pouvez sauvegarder la totalité des fichiers retrouvés ou juste quelques-uns depuis le panneau de gauche, en cochant la case *FileType List* ou celle de votre unité de stockage. La sauvegarde des fichiers ou répertoires sera possible sur unités de stockage optiques (CD/DVD/BD), mécaniques (disques durs) ou électronique (clés USB, cartes mémoire). L'avantage de GetData est de lire les informations sans apporter aucune modification sur les clusters. Pour réduire le recours à de telles applications, veillez à réaliser des sauvegardes régulières (au moins une fois par mois) de vos données précieuses sur au moins deux supports différents (disques optiques et disque dur, par exemple). Organisez vos fichiers dans des répertoires selon une logique objective, la recherche de « fichiers disparus » n'en sera que facilitée. **P.-E. Laurent**

AVIS D'EXPERT

Cet article permet de récupérer des pannes logiques, liées à des problèmes logiciels (suppression, formatage, etc.). Un disque dur victime d'un choc peut non seulement présenter des défaillances logicielles, mais également physiques. Le problème est alors plus grave et nécessite une réparation en salle blanche (réduisant toutes contaminations). Tout n'est pas perdu, mais il faut avoir recours à des sociétés spécialisées (Aigon, Chronodisk, CRDEP…). Et la note risque d'être salée : plusieurs centaines d'euros pour quelques dizaines de gigaoctets.

Release by TEAM-DZ

MATÉRIEL REQUIS
Windows 7 et Vista

NIVEAU
Moyen

QUESTION

Alors que vous vouliez utiliser un ancien document pour vous en servir de modèle, vous l'avez sauvegardé sous le même nom au lieu de l'enregistrer sous un autre nom après l'avoir modifié. Le document original est-il vraiment perdu ?

Récupérez une ancienne version d'un document

> Clichés instantanés Cliquez du bouton droit sur l'icône du fichier et choisissez la commande *Restaurer les versions précédentes*. La liste des versions du fichier s'affiche avec l'indication de la date de leur enregistrement. Sélectionnez une version et cliquez sur *Ouvrir*. Cliquez sur *Copier* pour enregistrer la version sélectionnée dans un dossier de votre choix. Dirigez-vous sur *Restaurer* pour remplacer le dossier ou le fichier actuel (et donc perdre la version actuelle au profit de l'ancienne version). Si vous avez supprimé le fichier ou si aucune version précédente n'est proposée, diquez du bouton droit sur l'icône du dossier contenant le fichier et choisissez, ici aussi, la commande *Restaurer les versions précédentes*. Les différentes versions du dossier s'affichent. Sélectionnez celle dont la date vous convient et cliquez sur le bouton *Ouvrir*. La fenêtre de l'Explorateur Windows affiche le contenu du dossier tel qu'il était à la date indiquée. Ouvrez le fichier qui vous intéresse et enregistrez-le ou copiez-le dans un autre dossier. Cette fonction *Versions précédentes* se base sur la Restauration système et sur la sauvegarde du système. La boîte de dialogue *Versions précédentes* affiche l'emplacement des versions : *Cliché instantané*, *Point de Restauration* (pour une version basée sur la Restauration système) ou *Sauvegarde*. La récupération à partir d'un point de restauration est instantanée puisque l'élément est déjà présent sur votre disque dur. La restauration depuis une sauvegarde déclenche un assistant qui vous guide pas à pas.

MATÉRIEL REQUIS
Internet Explorer

NIVEAU
Facile

QUESTION

Quand vous téléchargez un fichier, Internet Explorer demande de choisir le dossier de destination. Par défaut, il propose toujours le dossier dans lequel vous avez effectué le précédent téléchargement. Comment obliger Internet Explorer à toujours proposer le même dossier ?

Téléchargez toujours vers le même dossier

> Base de registre Ouvrez regedit, l'éditeur de la Base de Registre. Sélectionnez la clé *HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer* et double-cliquez sur la valeur *Download Directory*. Elle contient le chemin complet du dossier qui sera proposé lors du prochain téléchargement. Remplacez-le par le chemin d'un dossier de votre choix. Par exemple, si vous voulez que ce soit votre Bureau et si vous utilisez Windows Vista ou 7, entrez *C:\users\max\desktop* (en supposant que votre nom d'utilisateur est Max). Si vous utilisez Windows XP, voici le chemin du Bureau : *C:\documents and settings\max\bureau*. Lors du prochain téléchargement, c'est donc ce dossier qui sera suggéré. Vous avez le droit de le modifier mais c'est ce nouveau dossier qui sera enregistré dans la Base de Registre et donc proposé la prochaine fois. Pour empêcher toute modification de la valeur *Download Directory*, sélectionnez-la et choisissez la commande *Édition-Autorisations*. Cliquez sur le bouton *Avancé* (Windows Vista ou 7) ou *Paramètres avancés* (Windows XP). Sélectionnez votre nom d'utilisateur dans la liste et cliquez sur *Modifier*. Repérez l'autorisation *Définir la valeur* et cochez la case de la colonne *Refuser*. Validez en diquant sur *OK*.

À LIRE

Le registre Windows 7
Ce livre sur le registre s'adresse aux utilisateurs expérimentés. Il traite tout d'abord de l'architecture du Registre, des techniques pour administrer celui-ci à distance et des outils disponibles à partir de l'Invite de commandes. Il explique ensuite comment gérer les ressources réseau au moyen de scripts en utilisant notamment PowerShell. Le livre passe en revue les applications indispensables pour suivre l'activité du Registre et ses interactions avec le système.
Auteur Jean-Noël Anderruthy
Edition ENI
Prix 37 €

Release by TEAM-DZ

SOMMAIRE

CHANGEZ DE NAVIGATEUR
Pour booster internet, passez à Internet Explorer 8 (bientôt 9).

PROBLÈMES DE FILS ET DE MACHINES
L'accélération des accès internet passe par une installation propre.

VERS UN INTERNET 3.0
Un glissement des usages vers les applications hébergées dans le cloud.

L'ACCÉLÉRATION EXTERNE…
Il existe une méthode… c'est le serveur proxy.

ACCÉDEZ PLUS VITE À INTERNET

Un internaute peut-il accélérer son accès à internet? **En d'autres termes, aller plus vite que ce que peut offrir par défaut un fournisseur d'accès?** La réponse est généralement oui, à condition de faire des choix, et dépend essentiellement du type de service utilisé et du prix que l'on peut y consacrer. Isoler le poste de consultation des « encombrements » d'internet est une première étape.

Internet plus rapide qu'internet, est-ce possible? Théoriquement, non. Comment pourrait-on faire transiter plus d'informations que ne le permet le débit d'une connexion ADSL? Pourtant, en pratique, il est toujours possible d'améliorer les choses. Tout d'abord parce que l'accès internet idéal n'existe pas, pas plus que le réseau local idéal, le poste de travail idéal, la configuration idéale ou le protocole idéal. Des configurations par défaut inadaptées aux publicités et pop-up indésirables, en passant par les activités des virus, les câblages de mauvaise qualité, les filtrages imposés par certains opérateurs ou serveurs de données, on ne compte plus les accidents de parcours qui freinent ceux qui empruntent les autoroutes de l'information. Pour prendre cette route dans les meilleures conditions possibles, il faut tout d'abord posséder un véhicule qui « roule » bien, sans spywares téléchargeurs de réclames, sans problème de réseau local et sans accident de raccordement téléphonique.

Les débits restent liés aux distances de raccordement

Un bon câblage, un ordinateur propre et non surchargé, c'est parfois plus de 20 % de vitesse en plus et surtout un confort d'utilisation appréciable. Puis surviennent les problèmes routiers. Sur la Toile, tout le monde n'est pas logé à la même enseigne. Il y a ceux qui ont la chance d'habiter Paris, à deux pas des principaux échangeurs, et il y a ceux qui sont isolés des axes de grande circulation par 30 km de chemins de campagne: les abonnés au bas débit, les clients du ReAdsl, les abonnés en zone non dégroupée. Pour eux, il existe des moteurs d'appoint chargés d'accélérer soit la navigation dans l'espace web, soit le téléchargement, soit la réception des flux… Proxy, clients de téléchargement distants, tunnels chiffrés, si ces outils comblent en partie la fracture numérique qui sépare les internautes citadins et campagnards, ils sont tout aussi utilisables par les privilégiés de l'accès fibre optique ou ADSL 2+ « plein ». En France, les opérateurs, et notamment Free, poussent pour que le drainage de proximité dans les villes se fasse via un réseau de fibres, offrant une bande passante plus élevée et qui n'hypothèque pas les développements futurs et les besoins croissants en bande passante. La solution alternative, le VDSL qui est une évolution récente de l'ADSL, s'avère une technologie intéressante pour assurer les liaisons d'immeuble entre la « box » d'opérateur et un câblage fibre qui s'arrêterait au trottoir (« fibre to the curb »). Ce petit « pont » technologique est toutefois

Release by TEAM-DZ

conditionné par la présence de câble en cuivre de qualité. À lui seul, le VDSL peut quasiment doubler la vitesse d'accès au web. Cette réutilisation du câblage téléphonique, qui n'exige pas un tirage de fibres dans tous les appartements, possède des arguments évidents. Mais tout dépendra de la qualité de l'installation existante qui doit être du niveau d'un câble de catégorie 3 pour supporter le VDSL. En cas de remplacement, du fait de l'augmentation du prix du cuivre, la solution de la fibre optique sera devenue un meilleur investissement sur le long terme. **Dossier réalisé par M. Olanié et S. Belkhayat**

JARGON

Proxy Serveur distant à large bande passante chargé d'isoler le poste client (l'utilisateur) des problèmes d'encombrement réseau et de filtrer les données indésirables (publicité, pop-up, macros, etc.).

VPN Protocole de chiffrement servant à protéger le contenu d'un échange sur internet. Ce « masque » logiciel permet également de bloquer et contourner les « ralentisseurs de débit P2P » que certains FAI imposent à leurs abonnés.

Streaming Lecture d'informations audio ou vidéo en flux. Exemples : vidéos sur YouTube, Hulu.com, radios internet sur Shoutcast, etc.

Filtre maître Filtre de séparation situé en amont de la box d'opérateur destiné à séparer physiquement la ligne téléphonique des équipements informatiques en deux réseaux distincts. Il remplace la multitude de prises gigognes intégrant un filtre ADSL que l'on doit intercaler sur la ligne de chaque poste téléphonique.

Release by TEAM-DZ

Le navigateur, premier point de ralentissement

Si l'on ne devait donner qu'un conseil pour booster internet, ce serait celui-là : **changez de navigateur et passez à Internet Explorer 8 (bientôt 9), Google Chrome, Firefox…**

Longtemps, les navigateurs n'ont été que de simples interfaces HTML. Aujourd'hui, un browser s'apparente de plus en plus à un véritable système d'exploitation : langage intégré (scripts et interprètes divers, etc.), gestion des machines virtuelles Java, instances isolées dans des espaces mémoire compartimentés, sécurité accrue et bien sûr rapidité d'exécution améliorée.

Quelques astuces pour aller plus vite avec IE

Dans un premier temps, vous pouvez désactiver le filtre anti-phishing d'IE, qui compare les URL invoquées et celles d'une « liste noire » mise à jour par Microsoft (dans *Outils > Options Internet > Avancé > Filtre anti-hameçonnage*). Récupérez ensuite les 20 % de bande passante que Windows octroie par défaut pour ce filtre : exécutez *gpedit.msc*, puis déployez dans la fenêtre de cet outil les branches *Stratégie Ordinateur Local > Modèles d'administration > Réseau > Planificateur de paquets QoS* pour activer l'option *Limiter la bande passante réservable* et lui donner la valeur *0 %*. Passez à dix le nombre de téléchargements sous Internet Explorer, originellement limité à deux ou quatre sessions : activez le bouton *Fixit* accessible sur la page du Technet Microsoft : http://support.microsoft.com/kb/282402. Cette astuce permet de contourner les limitations de débit « par sessions » imposées par les serveurs de téléchargement et les fournisseurs d'accès. Autre « Fixit » intéressant : celui qui réinitialise les paramètres d'IE. Cet outil élimine également plusieurs causes d'arrêts inopinés du navigateur : http://support.microsoft.com/kb/923737.Plus un navigateur est utilisé, plus il est perclus de programmes annexes qui parfois abritent des virus. Un Fixit Microsoft conçu pour IE 8 les éliminera : http://support.microsoft.com/kb/976915. ■

Le VPN, un cas à part !

ZOOM SUR

> UN TUNNEL PARALLÈLE Un VPN, ou tunnel de liaison chiffré, n'est pas à proprement parlé un outil d'accélération du web. Il sert à camoufler, à l'aide d'un mécanisme de chiffrement, le contenu d'une communication entre le « proxy-VPN » et le poste client. Le proxy étant, dans la plupart des offres, situé en dehors du territoire français, il devient impossible à une instance juridique, policière ou toute autre officine de « deviner » ce qui transite dans ce tuyau. Mais cet outil d'anonymisation peut parfois servir d'accélérateur en masquant au fournisseur d'accès le protocole réellement utilisé à l'intérieur dudit tuyau. Certains FAI pratiquent en effet une chasse aux protocoles indésirables, pour des raisons de préservation de leur bande passante ou pour interdire certaines applications. Citons notamment tous les opérateurs de téléphonie mobile proposant des forfaits internet illimités mais qui bloquent certaines applications (VoIP, streaming…), ou les FAI qui, tel Free, ralentissent les échanges P2P de leurs abonnés situés en zone non dégroupée. L'usage d'un tunnel VPN empêche alors cette détection de protocoles interdits. Les services VPN, tout comme leurs cousins les proxy, sont proposés parfois en service gratuit mais limité (bande passante, protocole, durée de connexion…), et le plus souvent sous forme d'abonnement variant entre 5 et 20 euros par mois. Citons pour exemple vpnfacile.com, proxydaddy.net, perfect-privacy.com ou securenetics.com.

Release by TEAM-DZ

Résolvez les problèmes de fils et de machines

Les premiers pas vers une accélération **des accès internet passent avant tout par une installation propre** du réseau local informatique et de l'installation téléphonique.

En règle générale, les installations ADSL utilisent le câblage téléphonique déjà présent. Comme celui-ci n'est pas du tout étudié pour véhiculer des données « large bande/haut débit », ses multiples branchements et dérivations peuvent provoquer des pertes importantes du signal ADSL lui-même par rupture d'impédance ou plus simplement, du fait de la mauvaise qualité de connexions. En outre, un câblage téléphonique trop important peut jouer le rôle d'antenne radio et « capter », si l'on se trouve à proximité d'un émetteur en ondes longues : *France Inter* (162 kHz), *Europe 1* (183 kHz) ; le spectre d'une liaison ADSL 2+ couvre de 20 KHz à 2,2 MHz. D'autres générateurs peuvent perturber une installation ADSL : moteurs électriques, vélomoteurs dont les condensateurs d'antiparasitage ont succombé.

La qualité du signal dépend de l'infrastructure

À ces bruits impulsifs, on peut également ajouter les bruits d'écho généralement liés à un changement de calibre de médium (diamètre du câble téléphonique) et l'affaiblissement provoqué par des longueurs de fils de liaison trop importants. Les câbles ethernet de mauvaise qualité impacteront la qualité du signal ADSL. Un connecteur mal monté, oxydé ou cassé et assurant un mauvais contact provoquera immanquablement des accidents de transmission (nack). Si le phénomène passe souvent inaperçu entre PC d'un même réseau, des rejets incessants de paquets entre un ordinateur et la « box » d'opérateur diminueront (parfois jusqu'à 30 %) le débit reçu…

Des solutions souvent simples pour isoler les problèmes

Après avoir coupé le câble téléphonique au plus près de son point d'arrivée, insérez un filtre ADSL maître. Ce dernier isolera bien mieux la partie « informatique » de la section téléphonique que ne le feront les conjoncteurs-filtre fournis généralement avec les boîtiers d'opérateurs. Une élimination de l'installation téléphonique tout entière (au profit de postes sans fil Dect, par exemple) réduira considérablement les « effets antenne ». Dans certains cas de perturbation radio particulièrement difficiles, il peut être nécessaire d'ajouter un filtre de type « notch » en amont du câblage, dont la fréquence de coupure sera calée sur celle de l'émetteur indésirable. Un filtre maître est vendu entre 15 et 30 euros et résout généralement tous les aléas provoqués par l'installation téléphonique. Enfin, un raccordement de l'installation à une bonne prise de terre – les drainages « dernier kilomètre » effectués par l'opérateur historique ne sont pas toujours à la terre et aux normes – élimine très souvent des problèmes d'accrochage et de « boucle de masse ». Côté ethernet, surtout depuis que sont apparues les premières interfaces gigabit grand public, il est devenu totalement illusoire d'envisager de fabriquer soi-même des cordons de raccordement RJ45. En câblage 100 ou 1000Base-T, il est obligatoire d'installer des cordons surmoulés et certifiés achetés dans le commerce. Non pas pour « aller plus vite », le plus rapide des ADSL 2+ dans des conditions idéales (quasiment jamais atteintes) ne dépassera pas 24 Mb/s en flux entrant… une paille

À SAVOIR… Le VDSL, un accélérateur très spécial

> L'OBSERVATEUR D'ÉVÉNEMENTS On parle de lui comme d'un successeur d'ADSL 2+, d'un concurrent de la fibre moins cher et tout aussi performant. Lui, c'est le VDSL, pour « Very High Bitrate Digital Subscriber Line ». Et s'il peut battre de vitesse l'ADSL 2+ (55 Mb/s contre 22 Mb/s), ce n'est en aucun cas un rival du très haut débit par fibre optique (FTTH « Fiber to the home » ou FTTC « Fiber to the curb »). Ce serait même un excellent outil complémentaire. Historiquement parlant, le VDSL n'a pas décollé en France, alors que cette technique est courante notamment en Belgique et en Suisse. Bien adapté au milieu urbain, le VDSL exige que la distance entre la « box » et le DSLAM soit inférieure à 1 000 ou 1 500 mètres. Au-delà, l'atténuation dégrade trop le signal et l'ADSL 2 s'en tire bien mieux. C'est donc un drainage de proximité essentiellement adapté au milieu urbain. Or, en France, les opérateurs poussent pour que le drainage de proximité dans les villes se fasse via un réseau de fibres, offrant une bande passante plus élevée et qui n'hypothèque pas les développements futurs.

Release by TEAM-DZ

comparée aux 1000 Mb/s d'un réseau moderne. Mais un accident de réseau lié à un mauvais câblage pénalisera presque dans les mêmes proportions les données venant du routeur et celles reliant les différents ordinateurs du réseau. Si l'on peut se permettre de négliger une perte de 20 % de débit sur des échanges LAN, ces mêmes 20 % peuvent rapidement s'avérer exaspérant sur un flux DSL de 2 ou 3 Mb/s. Paradoxalement, un « bon » réseau Wi-Fi en 802.11a (5 GHz), utilisant une plage non perturbée du spectre, peut se montrer plus efficace avec ses 54 Mb/s partagés par trois ou quatre utilisateurs différents qu'une installation câblée de mauvaise qualité, même pilotée par un commutateur (switch) gigabit haut de gamme.

Second obstacle dans le parcours de l'utilisateur d'ADSL, l'informatique installée. Il n'est plus rare aujourd'hui de compter deux ou trois PC sur un réseau familial, sans oublier les serveurs, amplificateurs et autres lecteurs de DVD. Or, si tout ce petit monde parvient sans grande difficulté à cohabiter sur un réseau local, ce n'est plus du tout la même affaire lorsque chaque appareil tente d'accéder à internet. La récupération de l'inévitable lot de rustines Microsoft, chaque second mardi du mois, le téléchargement (légal) d'un film sous Creative Commons, une ou deux conversations VoIP… et brutalement la qualité de transmission se dégrade.

Les trois remèdes contre la congestion

À ce stade, les mesures d'urgence varient en fonction du type d'utilisation et des moyens financiers de chacun. Dans le cadre d'un réseau familial, le premier réflexe sera de déployer un firewall, un antivirus et un antirootkit sur chaque station et, par défaut, d'utiliser au moins ceux offerts par Microsoft. Sur une machine mal entretenue, les malwares et autres « add-in marketing » peuvent consommer jusqu'à 80 ou 90 % du temps d'occupation processeur d'un appareil, et par voie de conséquence rendre impossible tout travail sur la Toile. Les navigations sont ralenties, les téléchargements souvent impossibles en raison de certains filtres de « protection » mis en place par le virus ou l'addware lui-même. C'est donc avant tout une question de saturation de charge CPU plus qu'une question de surconsommation de bande passante internet. Une fois éliminés ces programmes parasites, le stade suivant consiste à établir une priorité aux différents types de communication. Priorité temporelle tout d'abord, la plus simple à mettre en œuvre : interdire le téléchargement de fichiers massifs ou les flux consommateurs non essentiels durant les heures de travail et vérifier l'extinction ou la mise en veille des ordinateurs des personnes absentes. C'est à la fois bon pour la planète et bon pour la salubrité du réseau qui ne risque pas d'être perturbé par des processus automatiques. Nul besoin d'outils sophistiqués, une simple entente entre usagers reste généralement suffisante. Si ces négociations échouent, il faudra recourir à un autre mode de classement prioritaire des flux, spatial et par type de protocole. Considérer par exemple que les conversations téléphoniques sont plus importantes qu'une session P2P d'échange de fichiers, que la télévision de 20 heures à 23 heures est prioritaire sur tout autre flux, ou qu'une sauvegarde nocturne sur un site distant via un FTP sécurisé ne devra être amoindrie que de 10 ou 20 % au maximum par un autre usage du net. Cette technique prend le nom de « gestion de la QoS » (gestion de la qualité de service). Une fonction qui ne peut se trouver qu'au niveau du premier équipement réseau situé au plus près de l'accès ADSL. À l'heure actuelle, aucune « box » d'opérateur ne comporte une telle fonction, et rares sont les routeurs du commerce qui intègrent ce genre de subtilité en standard. En revanche, la gestion de la QoS existe dans les principaux firmwares open source pour ces équipements de commutation et notamment dans plusieurs variantes d'OpenWRT.

Investissement pécuniaire et personnel

Recourir à ce genre de solution n'est pas gratuit. Il faut compter environ une cinquantaine d'euros pour un routeur compatible avec ce type de firmware. L'investissement le plus lourd est essentiellement intellectuel, puisque le paramétrage d'un équipement port par port, protocole par protocole, demande à la fois de la patience et une bonne connaissance des flux qui transitent entre le réseau local et internet. ■

Accès au net | Dérives et dépenses

■ Près de 500 euros par an S'il ne garde pas un œil rivé sur le compteur des dépenses, « l'homo informaticus » pourrait bien payer ses accélérateurs internet au-delà du raisonnable. Récapitulons : entre 50 et 400 euros annuels de service « proxy anti-publicité », 100 euros de client distant de téléchargement, éventuellement 100 ou 150 euros d'abonnement supplémentaire à un proxy géolocalisé facilitant l'accès à certains sites de streaming, comme Hulu.com, et l'on a alourdi de 300 euros le coût annuel d'un accès internet qui, en France, se situe aux environs de 480 euros. Lorsque plus de la moitié du coût d'un service reste constitué d'offres censées améliorer ledit service, on peut se demander si tout cela en vaut la peine. Ce qui pousse donc bon nombre d'internautes à « concentrer » certaines activités dans le temps. Les oubliés de l'ADSL, situés hors zone de couverture, sont quant à eux frappés d'une double peine. Au-delà du modem, ils ont l'obligation de payer un abonnement à un FAI aussi cher, sinon plus, qu'un accès haut débit, et d'autre part, sont dans la quasi-nécessité d'y adjoindre une offre de proxy filtrant. À ces dépenses, Il faut ajouter les frais fixes de mise à niveau du réseau local et de l'installation téléphonique. Vingt euros par-ci de filtre maître, 6 à 20 euros par-là par cordon réseau « certifié catégorie 6 », 40 ou 50 euros de commutateur gigabit, 50 à 1 000 euros de routeur Wi-Fi/Lan/Wan, modernisation de quelques cartes… Rapidement, un réseau familial constitué de trois ou quatre postes, un NAS, une machine multimédia et quelques appareils coûtera à son propriétaire administrateur entre 200 et 400 euros !

Release by TEAM-DZ

Vers un internet 3.0 basé sur les clouds

Avec la généralisation des applications P2P, **la déferlante des réseaux sociaux, la montée en puissance des offres de flux audio et vidéo à la demande,** on assiste à une très nette complexification des outils et protocoles utilisés sur internet.

La notion de proxy universel ou de « client Telnet distant », aussi vieille qu'internet lui-même et très largement antérieure à l'invention du web, a tendance à disparaître pour faire place à des proxy de plus en plus spécialisés, à des clients de plus en plus spécifiques, comme nous le montre la prolifération d'offres, telles Torrific, MegaUpload, FreeVPN, etc.

« Quelque part dans le nuage… »

Et c'est un peu comme si l'utilisateur perdait un peu plus chaque jour la maîtrise d'un internet libre et non-marchand. Pour télécharger plus rapidement : 5 euros par mois. Pour écrire un texte ou ouvrir un tableur : 20 euros par trimestre. Pour bénéficier de liaisons téléphoniques IP de qualité, ajoutez 10 euros… L'industrie en général et les prestataires de services français en particulier rêvent d'un monde qui renouerait avec le modèle de facturation à paliers multiples du défunt Minitel. Demain, tous les services en ligne seront gratuits… mais soit incomplets, soit plus lents. Pour le niveau supérieur, c'est un long glissement de l'ensemble des usages vers les applications hébergées dans le « cloud » (gratuites ou payantes). On connaît déjà Gmail, Hotmail, Yahoo! Mail, la nouvelle messagerie instantanée de Facebook, sans oublier les autres réseaux sociaux, et dans le domaine professionnel, l'externalisation des serveurs et parfois même des stations de travail : offres VMWare, Citrix, Terminal Serveur revendues par des prestataires de services XaaS (Architecture As A Service, Software As A Service, Infrastructure As A Service, etc.). À très brève échéance, une grande partie des outils que nous avions l'habitude d'installer sur nos ordinateurs ne se trouvera plus sur nos disques durs, mais perdue « quelque part dans le nuage »… Ce qui aura, ce qui a d'ailleurs déjà une première conséquence, la modification profonde de la nature des navigateurs. Ceux-ci sont devenus, depuis ces deux dernières années, des quasi-systèmes d'exploitation. La chose se vérifie avec Google Chrome Android, Internet Explorer, Safari, Firefox. Ce qui ne va pas sans poser quelques problèmes de sécurité !

Navigateur ou téléphone : vers la fusion des genres

Mais surfer sur le web ne se pratique pas seulement sur un ordinateur. Depuis l'apparition des téléphones intelligents, relativement abordables, les abonnés sont témoins d'une course au « service facturé » et au « filtrage bien tempéré » de la part des opérateurs. Pourquoi ? Pour deux raisons au moins : le désir de voir les offres de services du « online » compenser la diminution des gains de la téléphonie classique, et la difficulté d'assurer les offres en question sur un réseau qui ne s'avère pas toujours capable de faire face à cette montée en charge. Il est ainsi hors de question pour Orange de prendre le risque de voir passer une conversation sous Skype ! En revanche, face au succès d'Apple Store, tout sera mis en œuvre pour que s'ouvrent des boutiques de contenu et de services. Le second point est une conséquence du premier : il faut que le réseau soit capable de supporter de tels services dont la plupart repose sur un accès internet. Et c'est loin d'être le cas. En Europe, l'accroissement des données reste lié à l'utilisation des smartphones, comptant pour plus de 40 % dans la consommation totale des données. Ces « gros consommateurs de bande passante », qui ne représentent que 2 à 3 % de la base client, utilisent environ 30 % de la capacité du réseau contribuant ainsi à une dégradation du service pour la base utilisateurs complète. En d'autres termes, l'année 2011 marquera probablement la mort des forfaits illimités ou exception, verra leur volume de données plafonné. ■

Release by TEAM-DZ

L'accélération externe, seule arme efficace

Toutes les méthodes décrites **jusqu'à présent ne sont jamais qu'une manière d'utiliser un accès web au mieux-disant technique.** Le fait d'ailleurs de parler d'accélération ou d'amélioration de l'accès internet est un abus de langage.

Il serait préférable de parler d'optimisation de l'accès. Car il est impossible d'aller plus vite que le débit offert par le fournisseur d'accès. Il existe pourtant une méthode qui permet d'obtenir plus rapidement une donnée ou un lot d'informations. C'est le serveur proxy. Il n'accélère pas non plus le débit général du brin Wan, mais il améliore notablement un protocole en particulier… au détriment des autres. Comment fonctionne un proxy? Un peu comme un tampon de données ultraspécialisé. Il s'agit en fait d'un cache, d'un espace de stockage intermédiaire, qui a pour fonction d'une part de récupérer des données le plus rapidement possible, et d'autre part d'éliminer tout ce qui n'est pas essentiel à la compréhension de l'information en en retransmettant une version expurgée vers l'utilisateur.

Il faut éliminer les éléments superflus

Au passage, le proxy peut, comme c'est souvent le cas pour certains sites web, compresser une partie du contenu, notamment les données textuelles, en tirant profit du fait que la totalité des navigateurs disponibles sur le marché intègre un outil de décompression « en ligne » (Gzip). Lors d'un surf sur la Toile, on imagine donc bien que les publicités, la majorité des photographies, les pop-up, les appliquettes Java et autres gadgets HTML ne sont pas toujours utiles. Or, le poids binaire des publicités et des images que l'on trouve sur une page web constitue parfois plus de 90 % de ce qui est téléchargé par chaque poste de travail. L'équation est simple: si l'on ampute une page de 90 % de son contenu, on améliore de 90 % sa vitesse d'affichage. Mais cette technique demeure loin d'être parfaite. Si le proxy est installé sur le poste de travail que l'on souhaite accélérer, l'amélioration s'avérera totalement illusoire, puisque si les publicités et photos ne sont pas affichées, elles n'en restent pas moins téléchargées pour être ensuite éliminées localement. Pour être efficace, un proxy doit être installé sur un serveur distant, si possible équipé d'accès internet à très haut débit (plusieurs mégabits par seconde) afin de masquer les ralentissements que provoque

Proxy, VPN, passerelles: de purs espions

À SAVOIR…

■ L'OPEN SOURCE N'EST PAS INVULNÉRABLE La grande majorité des services VPN utilise un programme open source: OpenVPN. Si, dans plus de 70 % des cas, ces offres sont installées et gérées par des professionnels, les 30 % restants ne sont pas aussi fiables. On trouve des offres utilisant le protocole d'identification PPTP, qui reste vulnérable à une attaque par « l'homme du milieu ». L'autre risque (plus humain): certains hébergeurs de services proxy gratuits n'hésitent pas à surveiller les « surfs » de leurs abonnés dans un but marketing, pour glisser des publicités ciblées entre deux pages web visitées. Enfin, si les tuyaux de communication sont chiffrés, il reste bien plus rare que ce soit aussi le cas des disques sur lesquels sont « tamponnées » les données du proxy. En cas de demande des autorités du pays dans lequel réside l'hébergeur de services, les données des clients peuvent être saisies et examinées.

Release by TEAM-DZ

Sites | Montez votre propre proxy

La meilleure méthode Les services gratuits ou payants ne parviennent pas à vous satisfaire ? Vous possédez de bonnes bases techniques en informatique ? Fabriquez votre propre proxy. De manière très résumée, il « suffit » de louer un serveur hébergé dans le pays de votre choix (les prix oscillent entre 5 et 15 € par mois) et d'y installer un proxy filtrant (Squid, Polipo www.pps.jussieu.fr/~jch/software/polipo ou privoxy www.privoxy.org sous Linux Debian, par exemple). De nombreux conseils ainsi qu'une liste des sites publicitaires à bloquer est disponible sur yoyo.org (http://pgl.yoyo.org/adservers/index.php). La liaison avec ce serveur intermédiaire peut être perfectionnée par l'adjonction d'un tunnel chiffré, tel que OpenVPN (http://openmaniak.com/fr/openvpn_pki.php). Tous les outils mentionnés ici sont totalement compatibles avec un poste client sous Windows et Internet Explorer, toutes versions confondues.

immanquablement cette opération de « nettoyage des pages web ». Généralement, les proxys sont également doublés d'un programme de gestion de cache qui tente de calculer statistiquement les pages que l'usager risque de charger par la suite. Une technique qui, elle aussi, permet d'améliorer la vitesse d'affichage des pages. Bien sûr, ces services ne sont pas gratuits. Les offres non payantes sont généralement de très mauvaise qualité, et s'adressent de plus en plus à une clientèle en quête d'une passerelle d'anonymisation plus que d'un service d'accélération. Pis encore, c'est souvent parmi ces offres gratuites (voir payantes et situées dans certains pays de l'Est) que l'on trouve les plus dangereux diffuseurs de virus et spywares. La prudence exige de limiter le choix d'un « web-based proxy » en France ou sur le territoire américain, et après avoir effectué une enquête de réputation de ces sites sur différents forums d'utilisateurs. Les serveurs capables d'assurer un filtrage paramétrable de ce que l'on souhaite éliminer ou non (images, publicités, javascript, etc.) sont pratiquement tous payants sous leur forme la plus utilisable. Les Proxify (prestataire américain) et concurrents se vendent par abonnement, à raison de 30 à 40 euros par mois environ, tandis que certains (Proxyconn par exemple) facturent leurs services 60 dollars par an, avec strictement le même niveau de qualité. Une offre qui n'est étudiée que pour accélérer la visite des pages web, la récupération d'e-mails, la lecture des newsgroups et tout autre service reposant sur des contenus textuels. Il reste en revanche inefficace lorsqu'il s'agit de transférer des fichiers binaires « non redondants » (.exe, .zip, .mpeg, etc.). Car il n'y a rien à filtrer dans un tel fichier : ni publicité, ni image, et les algorithmes de compression classiques (Lempel-Ziv…) ne peuvent pas diminuer leur taille.

L'ASTUCE

ASSOCIEZ DEUX CANAUX

L'agrégation de ports Wan, soit l'utilisation de deux accès internet, si elle multiplie par deux la facture mensuelle ADSL, nécessite l'achat d'un routeur « double ports Wan ». Les prix oscillent entre 250 et 1 500 euros pour les appareils les moins chers. Mais ils assurent la supervision de la qualité de service (QoS), les fonctions d'antivirus-antispam et firewal. IS offre tout ce qui peut se faire en matière de « nettoyage internet », d'optimisation et de sécurité. Certains utilisateurs exploitent deux lignes d'opérateurs différents, ce qui réduit les risques d'arrêt total des communications.

Le téléchargement n'est pas gratuit non plus…

L'accélération du téléchargement utilise une logique légèrement différente… et, bien sûr, des services différents et également payants. Pour accroître la vitesse de récupération d'un fichier binaire à l'aide d'un proxy, il faut réunir trois conditions : que le logiciel de téléchargement (FTP, P2P, etc.) soit situé sur le serveur proxy, et non sur le poste de travail. Que ledit serveur possède un accès à très large bande passante afin que les temps de récupération de fichiers soient les plus courts possibles. Que le lien établi entre le poste client et le proxy soit également le plus rapide possible. C'est la réunion de ces trois conditions qui a fait le succès de sites tels que Torrific (ex-BTaccel), Burnbit, LeechPack et consorts ; ils possèdent tous la capacité de récupérer très rapidement des fichiers compte tenu de la taille des « tuyaux » qui les alimentent, et mettent ensuite à disposition les données récupérées en « téléchargement direct », bien plus rapide que via un protocole P2P. Coûtant entre 7 et 9 euros par mois en version « non limitée », ils donnent en outre à l'utilisateur le droit de récupérer plusieurs fichiers simultanément. Or, les contraintes de gestion de la bande passante imposées par certains FAI, voire parfois les limitations des outils utilisés, plafonnent le débit maximal d'une session « WebFTP ». Généralement aux alentours de 50 à 200 Kb/s en zone non dégroupée et en fonction de l'heure du jour, les zones dégroupées étant considérablement plus favorisées. En ouvrant une dizaine de sessions simultanées de ce type, il est alors possible de friser les 2 Mb/s… chose qui n'arrive jamais en temps normal. On peut alors réellement parler d'accélération du trafic sur internet. ■

Release by TEAM-DZ

Astuces express

MATÉRIEL REQUIS
Internet

NIVEAU
Facile

QUESTION

Vous recherchez des informations sur une personne ou une entreprise ? Google fournit beaucoup de renseignements, trop nombreux et surtout très désordonnés. Comment obtenir des résultats plus précis et structurés ?

Cherchez des personnes et des entreprises sur KGB people

> Un moteur spécialisé Le site internet KGB people (**www.kgbpeople.fr**) interroge les principaux moteurs de recherche, quelques plates-formes de blog, les sites de news, les réseaux sociaux, les sites de partage et ramène tout ce qu'il trouve. Si les résultats ne sont pas toujours exhaustifs (certaines informations sont privées ou enfouies dans des bases de données dont l'accès exige une identification), ils restent néanmoins pertinents. Entrez le nom et le prénom de la personne recherchée. Par défaut, la requête est limitée à la France, mais vous pouvez ouvrir la liste pour choisir un autre pays ou demander à ce que la recherche soit internationale (*Worldwide*). Cliquez sur le bouton *Recherche*. Les résultats sont distribués au travers de quatre sections : les réseaux sociaux, les moteurs de recherche, les données multimédias, les données personnelles. Le contenu de chaque section est accessible par l'intermédiaire de la barre d'onglets. Cliquez sur l'onglet d'un groupe de résultat. Le nom des outils et des sites consultés par KGB people apparaît dans des bandeaux. Dirigez-vous sur le bouton + d'un bandeau pour voir les données. Le titre des infos récoltées s'affiche. Cliquez sur le bouton + pour voir les détails. Pour communiquer le résultat d'une recherche à vos amis, utilisez le bouton *Partager ce résultat*. Vous avez alors la possibilité de choisir un réseau social ou encore l'envoi par e-mail.

MATÉRIEL REQUIS
Windows XP, Vista et 7

NIVEAU
Moyen

QUESTION

Comment accélérer le démarrage de Windows sans ouvrir les entrailles de la Base de Registre ni l'utilitaire de configuration système ? Et comment savoir quels éléments ralentisseurs peuvent être supprimés sans mettre en danger le système ?

Accélérez le démarrage de Windows avec Soluto

> Installez Soluto Téléchargez Soluto à partir de son site (www.soluto.com). Après l'installation, Soluto démarre automatiquement et propose de relancer le PC pour analyser la procédure de démarrage. Cliquez sur le bouton *Reboot Now*. Après le redémarrage, Soluto indique dans le coin inférieur gauche de l'écran la durée totale de la procédure.

> Examinez l'analyse du démarrage Lancez Soluto. Le logiciel affiche les applications qui ont été lancées au cours du démarrage. Elles sont classées dans trois catégories : en vert *No-brainer* (à supprimer), en orange *Potentially removable* (éventuellement à éliminer) et en gris *Cannot be removed* (à conserver car indispensables au système).

> Supprimez les programmes superflus Cliquez dans la barre verte puis sélectionnez la case d'une application. Dirigez-vous sur *More* puis sur l'un des trois boutons : *Pause* (l'élément n'est plus exécuté au cours du démarrage), *Delay* (l'élément est exécuté après le démarrage) ou *in Boot* (l'application reste dans la procédure de démarrage).

Release by TEAM-DZ

Sécurisez les droits d'accès à Facebook

Facebook a beau disposer de nombreux avantages, il ne faut surtout pas l'utiliser sans en modifier les réglages. **Par défaut, beaucoup de renseignements personnels y sont en effet publics.** Voici quelques conseils pour maîtriser les droits d'accès à vos données.

NIVEAU
Débutant

MATÉRIEL NÉCESSAIRE
- PC avec un accès à internet

TEMPS DE RÉALISATION
45 minutes

La mauvaise réputation de Facebook ne tient pas seulement aux déclarations désinvoltes de son fondateur au sujet de la vie privée des gens. Facebook incite ses utilisateurs à multiplier les contacts et à partager le maximum d'éléments pour qu'il puisse affiner le profil publicitaire de chacun. Les réglages par défaut des profils sont conçus exprès pour le partage tous azimuts et l'expression spontanée, ce qui peut poser des problèmes dans le cas d'une utilisation à la fois personnelle et professionnelle. Justement, Facebook est un réseau à tout faire. Les contacts (les « amis » Facebook) peuvent être des amis, d'anciens camarades de classe, des collaborateurs ou des relations amoureuses potentielles. Dans son profil, on peut indiquer son CV, ses opinions politiques et ses préférences sexuelles. Créer un profil par usage est possible, mais pas du tout pratique. On finit par n'utiliser que le plus fréquenté. Nous allons voir quels sont les subtilités et les pièges des réglages de confidentialité des profils, et définir une méthode pour compartimenter les infos entre les divers aspects de votre vie.

1 N'affichez pas votre liste d'amis Pour accéder aux réglages de Facebook concernant les droits d'accès à vos informations personnelles, cliquez sur le menu *Compte*, en haut à droite de la page d'accueil, puis sur *Paramètres de confidentialité*. Là, dirigez-vous sur le lien *Afficher les paramètres*, sous *Entrer en contact sur Facebook*. C'est ici que vous associez un type de contact à une action particulière, comme vous envoyer des messages ou voir votre formation. Chaque action peut être effectuée par vos amis, par les amis de vos amis ou par tout le monde. Dans ce dernier cas, les données sont accessibles à tout internet et en particulier aux sites partenaires de Facebook, aux applications tierces et aux moteurs de recherche. La diffusion de la liste d'amis peut poser problème, par exemple si vos amitiés politiques sont peu compatibles avec les opinions de votre employeur. Dans ce cas, il est prudent de restreindre l'accès à cette liste à vous-même, en choisissant l'option *Personnaliser*, puis *Moi uniquement*.

2 Limitez les informations sensibles Toujours dans les *Paramètres de confidentialité*, vous voyez d'un coup d'œil qui accède aux informations affichées sur votre profil. Certaines d'entre elles, apparemment anodines, comme la date de naissance et la ville d'origine, révèlent ensemble les neuf premiers chiffres de votre numéro d'identification de sécurité sociale. Les coordonnées téléphoniques ou l'adresse électronique ne devraient pas

PARAMÈTRES DE CONFIDENTIALITÉ
Très peu utilisés, ces paramètres vous permettent de restreindre l'accès aux informations à votre seul usage, via l'option *Personnaliser* puis *Moi uniquement*.

1

2

Release by TEAM-DZ

L'ASTUCE : GARE AUX LIENS SUSPECTS

Il n'est pas rare que les utilisateurs de Facebook reçoivent un message comportant un lien assorti d'un commentaire tentateur, du genre « Va voir là, c'est vraiment énorme ! ». Parfois, il ne s'agit que d'une attaque de type cross-site scripting, qui consiste à injecter dans le serveur des commandes héritant de vos droits d'accès. L'attaquant pourra ainsi polluer de spam vos amis, récupérer les données qui vous sont accessibles, changer votre mot de passe...

être accessibles à tout le monde, sauf si vous souhaitez recevoir du spam. La localisation géographique ou les photos sur lesquelles vous êtes identifié peuvent aussi se révéler utiles à des cambrioleurs, à des employeurs inquisiteurs ou à un conjoint jaloux. Le réglage recommandé par Facebook ne convient pas nécessairement à votre situation et il est souvent préférable de l'ajuster en suivant le lien *Personnaliser les paramètres* et en examinant la partie *Ce que je partage*. En dessous, dans *Ce que d'autres partagent,* vous pouvez contrôler (en partie) ce que vos amis peuvent diffuser sur vous. Facebook permet en effet d'identifier une personne sur une photo. La loi française oblige à recueillir au préalable l'accord de la personne en question, laquelle n'a aucun moyen technique de s'opposer à la diffusion ailleurs que sur son profil. Pour empêcher d'y afficher les photos sur lesquelles vous êtes « tagué », cliquez sur *Modifier les paramètres* en face de *Photos et vidéos dans lesquelles je suis identifié(e)* puis choisissez *Personnaliser > Moi uniquement*.

3 Les amis de vos amis ne sont pas vos amis

Outre les informations vous concernant, vous alimentez Facebook avec de nombreuses contributions : articles, liens, images, vidéos, commentaires. Ces contenus correspondent à *Vos statuts, photos et publications* du tableau des paramètres de confidentialité. À qui ouvrir des droits ? Quelques remarques : certains de vos « amis » Facebook peuvent être de parfaits inconnus. Que dire alors des amis d'amis ? Il vaut mieux autoriser l'accès à vos publications et photos aux seuls amis et, au cas par cas, élargir la diffusion d'un élément à l'aide du menu signalé par un cadenas et situé à gauche du bouton *Partager*. Cette dernière possibilité est apparue cet été. Un autre point doit attirer votre vigilance. Lorsque vous commentez les photos de vos amis, ce sont leurs réglages (qui vous sont a priori inconnus) qui s'appliquent à vos commentaires. Alors, ne vous lâchez pas totalement.

4 Classez vos amis dans des listes

Pour attribuer plus justement des droits d'accès, vous devez vous familiariser avec la fonction des listes d'amis de Facebook, pour classer vos relations par degré de proximité (famille, proche, connaissances), centres d'intérêt ou de type d'activité (loisirs, associatif, professionnel). Dans le menu *Compte*, cliquez sur *Gérer la liste d'amis*. Vous pouvez alors créer des listes d'amis et inclure une même personne dans plusieurs listes. Vous aurez ensuite la possibilité de ne montrer vos publications qu'aux personnes incluses dans vos listes. Pour cela, cliquez dans le menu attaché à chaque publication (représenté par un cadenas) puis choisissez *Personnaliser > Certaines personnes* et tapez le nom de votre liste.

5 Cachez vos publications à certaines personnes

La fonction d'exclusion, relativement récente, utilisée en conjonction avec les listes, permet au contraire de ne pas montrer vos publications à certains de vos amis. Dans *Personnaliser > Certaines personnes*, une ligne accueille les personnes ou listes à exclure de l'accès à tel ou tel élément. Comme il n'est pas évident d'y penser à chaque publication, il vaut mieux procéder à des réglages sensés dans les paramètres qui s'appliquent par défaut.

6 Attention aux applications

Au fil du temps, Facebook renforce son caractère de plate-forme d'applications à usage « social ». La dernière innovation s'appelle Opengraph. Il s'agit d'un protocole d'échange couplé à un traitement sémantique permettant d'étendre certaines fonctions de Facebook à d'autres sites web. Ainsi, le bouton *J'aime* fonctionne sur les sites adaptés et permet de partager entre amis des recommandations, sur un élément précis de la page, comme un livre, un auteur, un titre de musique. L'extension du domaine de Facebook rend d'autant plus nécessaire le contrôle de chaque application dans *Compte > Paramètres de confidentialité > Applications et sites web*.

Philippe Roure

Release by TEAM-DZ

Dopez Windows Mobile 6.5 avec Opera 10

Les capacités de transfert à haut-débit **des réseaux de téléphonie mobile alliées aux offres d'accès illimité à internet méritent** de disposer d'un navigateur web performant sous Windows Mobile 6.5. Opera Mobile 10 a toutes les qualités requises.

NIVEAU
Intermédiaire

MATÉRIEL NÉCESSAIRE
- Smartphone tactile sous Windows Mobile 6.5.x
- Connexion Wi-Fi et/ou 3G
- Opera Mobile 10

TEMPS DE RÉALISATION
25 minutes

Dans la foulée de l'iPhone d'Apple et de Google Android, Windows Phone 7 a pris lui aussi le train des smartphones « toujours connectés ». Sur le plan technique, le retard accumulé n'est qu'apparent, tant sont solides les bases sur lesquelles s'appuie l'environnement logiciel de Microsoft. Il n'est pas obligatoirement nécessaire de disposer de Windows Mobile 7, la dernière génération du système, pour révéler toute la puissance et l'adaptabilité d'une structure logicielle qui a déjà donné la preuve de sa pérennité. Les appareils fonctionnant sous Windows Mobile versions 6.5.x et 6.1, les plus nombreux actuellement en service, recèlent en matière de connexion à internet, d'énormes réserves qui ne demandent qu'à s'exprimer. Mais il faudra que l'utilisateur fasse l'effort de remplacer l'ancienne version d'Internet Explorer Mobile fournie d'office par un navigateur web de dernière génération, Opera Mobile 10 par exemple.

1 Une mosaïque de sites proposée à l'ouverture

Plutôt que de charger une page d'accueil pointant vers son propre site ou celui d'un moteur de recherche, Opera Mobile 10 propose, en tant qu'écran d'accueil, une mosaïque de favoris. À la base, cinq destinations sont préremplies. La personnalisation de cette ressource est évidemment plus que recommandée.

Pour changer une destination déjà enregistrée, gardez le doigt ou le stylet appuyé sur sa représentation miniature. Après trois secondes, un menu à deux options apparaît : *Effacer ou Éditer*. En sélectionnant cette dernière, la liste des derniers sites visités apparaît. vous pouvez soit choisir l'une de ces références, soit taper une nouvelle adresse dans la barre supérieure. Appuyez ensuite sur le lien intitulé *Ajouter,* situé au bas de l'écran.

2 Une navigation plus simple donc plus efficace

L'écran de démarrage d'Opera Mobile 10 présente : en haut, une barre

ZOOM : INSTALLEZ L'APPLICATION SANS PC

Si la version 11 du navigateur Opera mérite d'être essayée sur PC, sa déclinaison mobile Opera 10, destinée aux smartphones équipés de Windows Mobile 6.5, donnera un coup de jeune à des mobiles pourtant récents. Le meilleur moyen d'accéder à la version adaptée à votre smartphone consiste à se connecter en employant le navigateur de base de l'appareil au site : m.opera.com. L'application est récupérée sous la forme d'une archive (.cab) qui peut être installée immédiatement. Le téléchargement sur PC, en revanche, oblige de repasser par ActiveSync, une opération plus lourde.

Release by TEAM-DZ

d'adresses et un champ de saisie permettant d'interroger le moteur de recherche Google, dans la zone centrale, la mosaïque des neuf favoris et en bas, des icônes de pilotage de l'application. En vous servant du stylet, pointez dans l'un des champs de saisie. L'écran se recompose pour faire apparaître le clavier virtuel de Windows Mobile tandis que le lien *Aller* (barre d'adresses) ou *Rechercher* (Google) s'affiche au bas de l'écran. Saisissez une adresse. L'opération est sensiblement facilitée, les trois lettres www apparaissant en tête de ligne par défaut. Une fois ce choix validé, le navigateur entame le chargement de la page.

3 Exploitez la navigation à onglets

Dès le chargement de la première page d'information, il est possible de tirer parti des possibilités de Opera Mobile 10, notamment en s'appuyant sur son système d'onglets pour charger plusieurs services en ligne simultanément. Pour cela, appuyez sur l'avant-dernière icône située à droite sous l'écran. Deux miniatures au minimum apparaissent, la dernière étant systématiquement grisée. Appuyez sur celle-ci sans la relâcher pour ouvrir un nouvel onglet par défaut, positionné sur la page des favoris. Barre d'adresses, de recherche, miniatures... Tout est bon pour lancer une nouvelle session pendant que, dans l'onglet précédent, les données terminent de se charger.

4 À la découverte des principaux réglages

En appuyant sur la dernière icône située sous l'écran à droite, vous faites apparaître le menu des outils. Comme dans le reste de l'application, l'interface est entièrement graphique, présentant cette fois des boutons. Sélectionnez l'option *Réglages*. Une liste de fonctions s'affiche alors. Selon les besoins, il est possible de mettre en service les principales fonctions d'aide à la navigation. En cas de connexion à des réseaux à bas débit, n'hésitez pas, par exemple, à interdire le chargement des images. La fonction *Turbo* peut en revanche toujours rester allumée (elle permet de compresser les données pour accélérer le chargement des pages). L'option *Affichage mobile* peut être mise en et hors service, selon que l'on souhaite ou non consulter les versions abrégées (dites « mobiles ») des sites visités.

5 Sauvegardez les pages visitées sur l'appareil

La sauvegarde des pages est une fonction rarement supportée par les navigateurs présents en standard sur les smartphones. Pour l'exploiter dans Opera Mobile 10, passez par le menu *Outils* et choisissez l'option *Pages enregistrées*. Vous voyez alors s'afficher la liste des documents déjà sauvegardés tandis que la première ligne permet d'enregistrer le site chargé dans l'onglet actif. Toujours dans le menu *Outils* mais au-dessus du bouton *Précédent* se trouve l'historique de navigation. Il permet par exemple de peupler rapidement un nouvel onglet en retournant sur un site précédemment visité. Vous pouvez aussi, pour plus de confidentialité, effacer l'historique en appuyant sur le bouton *Supprimer* (*Suppr. tout*) situé au bas de l'écran.

Thierry Pigot

GAGNEZ LA BATAILLE DU MULTIMÉDIA MOBILE Avec des opérateurs qui proposent des offres d'abonnement à la télévision mobile, le multimédia est le principal axe de concurrence qui se dessine pour les mois à venir. Si les tablettes tactiles ont l'avantage de disposer d'un grand écran pour profiter des services de vidéos à la demande, les smartphones ont pour eux la légèreté en ce qui concerne l'accès aux séquences présentes sur internet, notamment via YouTube et Dailymotion.
La prochaine barrière à franchir consiste à supporter les formats audio/vidéo les plus courants dont, notamment, les séquences au format flash conçu par Adobe. Une révision d'Opera Mobile 10 devrait rapidement apporter la compatibilité avec ce type de séquences multimédia, puisque des versions bêta sont déjà en cours de test. Le menu *Outils* dans l'option *Réglages* puis *Avancé* comporte une section consacrée aux plug-in. Cette disposition devrait rapidement permettre d'ajouter de nouvelles fonctionnalités. Une autre initiative des développeurs d'Opera Mobile 10 consiste à supporter une communauté en ligne afin de proposer des fonctions de réseau social mais aussi de favoriser la diffusion des nouvelles fonctionnalités au gré de leur apparition.

Release by TEAM-DZ

Sécurisez Windows Live Essentials 2011

Avec Windows Live Essentials 2011, **Microsoft propose onze outils pour tirer parti de ses services en ligne.** Voici comment en sécuriser l'utilisation tant du point de vue des données personnelles que du réseau.

NIVEAU

Débutant

MATÉRIEL NÉCESSAIRE

- Windows Live Essentials 2011
- Windows 7

TEMPS DE RÉALISATION

30 minutes

Intimement liés au réseau, les outils du pack Windows Live Essentials possèdent, à différents niveaux, des paramètres pour en améliorer la sécurité ou préserver vos données personnelles. Voici, application par application, la manière d'utiliser les bons paramètres.

Windows Live Essentials est un pack de logiciels téléchargeable à l'adresse explore.live.com. Pour l'installer il suffit d'exécuter le fichier *wlsetup-web.exe* en cliquant sur *Télécharger*. Vous y trouverez les nouvelles versions de Live Mail, Live Messenger et son complément, Live Mesh ainsi que Live Galery, Live Writer, la barre de navigateur Bing, le contrôle parental, Outlook Connector et Movie Maker. Silverlight, le concurrent d'Adobe Flash, fait aussi partie du lot. La sécurité de ces applications est à envisager sous trois angles : le premier est évidemment la mise à jour de chaque composant. Vient ensuite la sécurité réseau. Même si, sur ce point, les applications sont toutes pré-configurées de manière sécurisée, leur utilisation demande de suivre quelques impératifs. Enfin, la protection des données personnelles est à prendre en compte puisque plusieurs outils permettent de partager des données avec d'autres personnes, voire avec tous les internautes.

1 La barre de navigation Bing Elle s'insère en haut de la fenêtre du navigateur Internet Explorer. Elle permet notamment de s'assurer de la sécurité du navigateur. Pour faire apparaître le centre de sécurité, diquez sur l'icône verte à droite de la barre d'outils de Bing. Dans la fenêtre qui apparaît, vous pourrez voir l'état des protections *Blocage des fenêtres publicitaires*, *protection anti-hameçonnage* et *Sécurité de site* (il s'agit du fitre Smartscreen). Tous ces éléments doivent être actifs pour que votre navigation profite des sécurités d'Internet Explorer. Enfin, en diquant sur l'icône *Privé*, vous accéderez directement à la navigation « inprivate » sous Internet Explorer, qui ne laisse aucune trace de votre surf sur l'ordinateur.

ASTUCE : LE CONTRÔLE PARENTAL

Windows Live Essentials propose un système de contrôle parental. Une fois installé, vous devrez créer des comptes pour chaque utilisateur. Inscrivez *Créer un compte* dans le champ *Rechercher* du menu *Démarrer* de Windows. Une fois que vous aurez créé ces comptes (avec mot de passe) vous pourrez gérer les sites accessibles de votre ordinateur par tel ou tel utilisateur. Le contrôle peut aussi s'effectuer sur Live Messenger en acceptant tel ou tel contact dans la liste de vos enfants/adolescents.

Release by TEAM-DZ

VOTRE VIE PRIVÉE AVEC WINDOWS LIVE La sécurité passe aussi par la maîtrise des informations personnelles. Cet élément est de plus en plus crucial. Chaque outil proposé par cette suite est relié à votre profil Windows Live. Rendez-vous à l'adresse **windows.live.com**, identifiez-vous avec votre Windows Live ID si ce n'est pas fait. Cliquez ensuite sur votre pseudonyme, qui apparaît en haut à droite du site et choisissez *Paramètres de confidentialité*. Cette page fait apparaître l'ensemble des éléments que vous pouvez publier sur votre profil live et leur accessibilité. Cliquez sur *Afficher les paramètres actuels* pour pouvoir les modifier. Dans la partie *Information de base*, vous trouverez notamment *Information me concernant*, *Études* et *liste d'amis*. Nous vous conseillons le paramètre *Mes amis*. Par défaut, les nouveaux albums photos de Skydrive sont partagés avec tous vos amis. Là aussi, vous pouvez limiter ce paramètre à *certains de vos amis*… Enfin, dans la rubrique *Personnes pouvant me contacter*, vous pouvez régler *Invitation d'amis et de groupes* sur *Personne*. Dans ce cas, vous ne pourrez alimenter votre liste de contact qu'en les invitant. Une fois que vous aurez paramétré ces éléments, n'oubliez pas de diquer sur *Enregistrer* au bas de cette page.

2 Messenger : méfiez-vous des malwares

La sécurité dans Windows Live Messenger dépend surtout de son usage. Tout d'abord, il faut savoir que de nombreux malwares utilisent cette plate-forme pour trouver de nouvelles victimes. Le scénario classique est le suivant : un de vos contacts vous envoie un lien. Ce dernier abouti sur un site web qui va soit infecter votre machine en exploitant une faille de votre navigateur ou un de ses composants, soit vous proposer le téléchargement d'un fichier comportant un virus. Pour éviter cela, ne cliquez pas sur un lien qui vous est conseillé en anglais par une personne francophone… ou qui est hors ligne lors de l'envoi du message. Live Messenger étant relié à votre espace Windows Live, vous devrez aussi paramétrer les accès pour protéger vos données personnelles (voir l'encadré « zoom »).

3 Partagez en toute sécurité avec Live Mesh

Live Mesh est un outil de synchronisation. Il permet de copier le contenu d'un répertoire vers un autre ordinateur de façon quasi instantanée. Deux fonctions sont à surveiller pour la sécurité de cette application. Live Mesh permet de partager les répertoires avec d'autres utilisateurs. Le partage dans Live Mesh donne aussi accès aux ordinateurs à distance. Il convient donc tout d'abord de bien réaliser les mises à jour lorsque Microsoft les propose. Ensuite, lors de la synchronisation d'un répertoire, ce dernier est uniquement partagé avec le propriétaire du répertoire. Ouvrez Live Mesh et cliquez sur l'un des répertoires partagés. Dans *Partagé avec* doit figurer *Moi uniquement*. Cliquez sur cet élément si vous voulez le partager avec d'autres contacts. Entrez son adresse mail et choisissez ses droits. Si vous lui accordez les droits de modifier les autorisations, cet utilisateur pourra ajouter d'autres contacts dans le partage sans votre consentement. Pour vérifier l'état du système d'accès distant à votre ordinateur, cliquez sur *Distant* dans l'interface principale. Par défaut, cette fonction est désactivée.

4 Filtrez votre courrier dans Live Mail

Live Mail est le client e-mail des outils Live Essentials. Comme pour tous les clients mails, les problèmes de sécurité se situent dans les courriers reçus. Ouvrez le premier onglet de Live Mail, rendez-vous sur *Options* puis diquez sur *Options de sécurité*. Dans l'onglet *Option* de cette fenêtre, vous pouvez choisir le niveau de détection du courrier indésirable. Le niveau *élevé* est le plus pertinent. Nous vous conseillons aussi de cocher la case *Signaler le courrier indésirable à Microsoft* pour enrichir la base de données contre le spam. Vous pouvez aussi éliminer le spam en filtrant les e-mails selon leurs origines dans l'onglet *International*.

5 Spécifiez les droits d'accès de la galerie photo

Même si ce n'est pas évident, la galerie Live doit aussi faire l'objet d'attention. En effet, elle permet de publier vos documents, notamment sur Skydrive et Facebook. Veillez, lors de la création d'un nouveau dossier, à préciser les droits d'accès. Un accès public rendra toutes les photos présentes accessibles à tous les internautes. **Jean-Philippe Bay**

2

3

4

5

Release by TEAM-DZ

Installez le contrôle parental de SFR

SFR

20 minutes

Difficulté

Installer un logiciel de contrôle parental, c'est limiter aux jeunes internautes l'accès à des sites à caractère violent, pornographique ou raciste et empêcher le téléchargement de fichiers pirates.

MODE D'EMPLOI EN 8 ÉTAPES

1

Installez le programme La toute première chose à faire est de vous rendre à l'adresse suivante (http://securite.sfr.fr/telechargement.html) pour y télécharger gratuitement le logiciel de contrôle parental mis à disposition par SFR. Il est disponible en versions Mac et PC (Windows 2000/XP/Vista 32 et 64 bits et 7 en 32 bits uniquement).

2

Désactivez la sécurité Windows Il se peut que vous ayez à désactiver temporairement votre antivirus pour que l'installation se passe sans problème, et éventuellement l'ancienne version du logiciel incluse dans les SFR Pack Sécurité V8 et V9, si vous étiez déjà utilisateurs des solutions de protection de l'opérateur.

3

Profil de la cible Pendant la phase d'installation, le logiciel va vous demander deux choses. La première, et certainement la plus importante, est de choisir un mot de passe administrateur pouvant être complété par une question secrète. Celui-ci va vous être envoyé par courriel pour vous permettre de le retrouver facilement.

4

Public cible La seconde question se résume au choix du profil de l'utilisateur. Le programme vous propose ici deux types de profils préconfigurés : enfant ou adolescent. Les paramètres de verrouillage sont pour chaque parfaitement adaptés au public cible. Les contraintes ne sont pas les mêmes.

Release by TEAM-DZ

Relancez l'ordinateur Une fois l'installation terminée, redémarrez l'ordinateur. Faites-le sans hésiter, pour que le logiciel de contrôle parental puisse passer en mode actif et pour que vous puissiez avoir accès à la console d'administration, ce qui ne sera pas le cas tant que le PC n'aura pas redémarré.

Paramétrez l'outil La configuration du logiciel de contrôle parental se fait par le biais d'une interface web. Cette dernière est volontairement dépouillée pour gagner en lisibilité et en efficacité. En cliquant sur *Configuration*, vous pouvez activer ou désactiver et appliquer le contrôle parental à un seul compte utilisateur du PC.

Verrouillez les sites néfastes Vous avez la possibilité à tout moment d'accéder à un paramétrage avancé du contrôle parental. Dans l'interface web, cliquez sur l'onglet *Configuration avancée*. Vous pouvez ici ajouter des sites que vous jugez néfastes pour vos enfants, et auxquels ils n'auront pas accès.

Définissez des plages d'utilisation Si vous êtes dubitatif quant à l'efficacité des critères de filtrage appliqués dans les profils, rien ne vous empêche de les modifier selon vos propres paramètres. Vous pouvez aussi définir les jours et les plages horaires pendant lesquels l'internaute sera autorisé à surfer.

CE N'EST PAS LE CHOIX QUI MANQUE

Devant l'insistance de la loi Hadopi à ce que les particuliers se dotent le plus rapidement possible d'un système de filtrage efficace, les fournisseurs d'accès à internet ne sont pas les seuls à proposer un logiciel de contrôle parental. Les éditeurs de suites de sécurité les intègrent, progressivement pour certains, depuis quelque temps déjà pour d'autres, à leur produit. Ce qui est parfaitement logique, puisqu'au même titre qu'un antivirus ou un pare-feu, le contrôle parental s'inscrit dans le schéma de la protection totale de l'ordinateur et de la vie privée. Mais si vous êtes déjà équipé d'un antivirus et d'un pare-feu et que vous rechignez à acquérir une suite de sécurité à 70 euros pour bénéficier du contrôle parental, alors vous pouvez vous tourner vers des solutions tierces moins coûteuses. Parmi les rares logiciels francophones, citons Horaire PC (**www.horaire-pc.com** - 28,90 €). Il ne s'agit pas d'un logiciel de filtrage à proprement parler, mais plutôt d'un outil permettant de limiter le temps passé en navigation ou sur certains logiciels chronophages nécessitant une connexion internet. Dans la même veine que le logiciel proposé par SFR, on trouve, également en langue française, l'excellent Xooloo (29,99 €), logiciel de contrôle parental utilisé par le fournisseur Numericable.

Release by TEAM-DZ

Isolez le navigateur pour éviter les virus

Virtualbox

120 minutes

Initié

Les techniques de virtualisation de système sont devenues matures en quelques années. L'utilisateur peut les mettre à contribution pour sécuriser sa navigation sur le web.

IL VOUS FAUT AUSSI...

- ✔ Un deuxième OS
- ✔ un compte Google
- ✔ 2 Go de mémoire
- ✔ Un processeur Intel VT/AMD-V

Les programmes nuisibles entrent dans les ordinateurs par des voies diverses. Il y a longtemps, la disquette et les BBS étaient les principaux vecteurs. Récemment, les réseaux sociaux et les clés USB ont gagné la faveur des vixers (auteurs de virus et autres malwares). En dépit d'efforts visant à les rendre plus résistants aux injections de code viral, les navigateurs restent des cibles particulièrement exposées. Ils acceptent du Flash, du Javascript et des fichiers PDF d'origine indéterminée et ne sont pas tous isolés du système par d'infaillibles sandboxes. L'idée de notre montage est de créer, avec le logiciel Virtualbox, une machine virtuelle sans état. Dans cette machine virtuelle, vous installerez un système dit « invité » réservé à la navigation sur le web. Il sera relativement aisé de réduire la surface d'attaque d'un tel système, réduit à quelques fonctions. Mais surtout, un malware injecté au cours de la navigation ne pourra se propager automatiquement au système hôte, ni subsister dans le système invité à son prochain redémarrage. Vous devez cependant noter qu'un navigateur infecté en début de session serait dangereux à utiliser pendant la durée de celle-ci. En particulier, si vous devez communiquer des mots de passe ou un numéro de carte bancaire.

Avant de vous lancer, vous devez vous assurer que le matériel pourra faire tourner simultanément l'hôte qui accueille Virtualbox et l'invité logé dans la machine virtuelle. Avec moins de 2 Go, et sans un double cœur, mieux vaut éviter Windows 7 et préférer Windows XP SP3 ou même Linux en position d'invité. Les machines récentes disposent souvent d'une prise en charge matérielle de la virtualisation, qui accroît la vitesse et la fiabilité de ces opérations. Si le processeur possède des instructions Intel VT/AMD-V, assurez-vous qu'elles sont activées dans le BIOS. Le disque doit avoir au moins 20 Go de libre sur un système de fichiers NTFS. Sur le site www.virtualbox.org, choisissez la version de Virtualbox correspondant à son système hôte, 32 ou 64 bits. Pour installer un invité 64 bits sur un système hôte 32 bits, il faut un processeur 64 bits avec instructions VT/AMD-V. **Philippe Roure**

MODE D'EMPLOI EN 6 ÉTAPES

Créez une machine virtuelle Un clic sur le bouton *Créer* lance la procédure de création assistée. Les dialogues successifs demandent le type de système (Assurez vous d'en avoir la licence), la quantité de mémoire et l'espace disque. Le programme suggère des quantités compatibles avec le système sélectionné.

Configurez la machine invitée Avec la souris, sélectionnez la machine virtuelle dans la liste et cliquez le bouton *Configuration*. Dans l'onglet *Système*, vous pouvez attribuer plus d'un processeur virtuel (avec les instructions VT-x/AMD-V). Pour activer le partage de fichiers, dans l'onglet de *Répertoire partagé*, choisissez un répertoire sur l'hôte.

Release by TEAM-DZ

3

Installez le système Dans *Stockage*, assurez-vous que le lecteur de DVD contenant le média d'installation du système est bien pris en compte et visible. Si vous employez une image de ce média, sélectionnez le lecteur *Vide*, puis dans les attributs (à droite), déroulez le menu en forme de CD et choisissez un fichier de CD virtuel.

4

Installez les logiciels Lancez la machine virtuelle en appuyant sur *Démarrer* puis installez le navigateur et tous les modules nécessaires. Procédez aux mises à jour de sécurité du système et des logiciels. Limitez-vous au nécessaire. Redémarrez le système invité pour que les correctifs prennent effet et lancez le navigateur.

5

Prenez un instantané Prenez un instantané (menu *Machine* > *Prise d'un instantané*). Ensuite seulement, vous pouvez naviguer sur le web. À la fin de la session, fermez le système invité à partir du menu *Machine* > *Fermer* et non depuis le système invité. Dans la fenêtre qui s'ouvre, cochez la case *Revenir sur l'instantané actuel*.

6

Partagez des fichiers avec l'hôte Depuis le système invité, ajoutez une connexion à un lecteur réseau. Le nom du lecteur est *\\VBOXSVR*, auquel vous greffez le nom du répertoire partagé sur l'hôte (défini à l'étape 2). Vous pouvez ensuite choisir ce répertoire pour le téléchargement des fichiers.

AVEC OU SANS ÉTAT ?

Revenir au dernier instantané après chaque session est efficace contre les bots et troyens persistants mais présente quand même quelques inconvénients. Par exemple, garder le système invité à jour nécessite de suivre une procédure stricte. Juste après le démarrage de l'invité et avant de naviguer, appliquez les correctifs de sécurité, puis redémarrez. À ce moment, prenez un nouvel instantané. À la longue, vous devez faire le ménage dans les instantanés pour libérer de l'espace sur le disque, en supprimant les plus anciens.

Avec un système invité sans état, vous perdez aussi l'historique des sites visités et les marque-pages. Pour les conserver, le plus simple est de recourir à un service en ligne de synchronisation et de partage d'URL favorites. Google Bookmarks (Favoris Google) est un des plus simples et des plus fiables. Son module, installé avec la barre d'outils Google, est optionnel. En son absence, vous pouvez enregistrer manuellement une URL sur le site **www.google.com/bookmarks**, après vous être connecté à votre compte Google. Sur la page des Favoris Google, remplissez les champs du nom, de l'URL (copiée dans la barre d'adresse), des libellés et des notes. L'enregistrement est complété par l'action du bouton *Ajouter aux favoris*.

À la longue, vous pourrez être tenté d'abandonner ce dispositif que vous jugerez trop lourd et disproportionné par rapport à des risques pas toujours faciles à évaluer. Il est vrai que pour accéder exclusivement à des sites d'information, Wikipedia ou de la presse en ligne, cet arsenal est un petit peu surdimensionné. Mais le problème est là : le navigateur est aussi bien employé pour accéder à des sites à faible risque qu'à d'autres, nettement plus sulfureux. La solution est peut-être dans la séparation des genres.

Le navigateur « normal », intégré au système hôte, sera affecté aux travaux quotidiens et aux sites très sécurisés tandis que son double virtuel sera réservé au commerce en ligne (une cible favorite des pirates qui y placent des chevaux de Troie) et autres sites sensibles.

Release by TEAM-DZ

VBScript : Prenez le contrôle de votre système

Dans la panoplie des outils d'automatisation de Windows, on trouve le langage VBScript. **Directement dérivés du Visual Basic, les scripts VBS sont destinés à automatiser certaines tâches,** comme la copie de fichier ou le contrôle du navigateur.

NIVEAU
Expert

MATÉRIEL NÉCESSAIRE
- Windows Vista/7

TEMPS DE RÉALISATION
40 minutes

Windows, le système d'exploitation de référence pour les PC, accueille des millions d'applications différentes. Mais c'est aussi une plate-forme de développement pour ce que l'on appelle les scripts, programmes qui permettent d'effectuer des milliers d'actions sur le système ou sur des applications installées. Le langage de création de script le plus utilisé sous Windows est le VBScript. Directement dérivé du Visual Basic, ce langage permet de manipuler des fichiers et de lancer des programmes. Il est assez simple à maîtriser et propose une structure avec des variables, des boucles de contrôle et des manipulations d'objets. Le VBScript peut fonctionner dans plusieurs contextes : à l'intérieur de Windows (Windows Script Host), dans une page HTML ou encore au sein d'un serveur web de type IIS. Dans ce guide pratique, nous vous proposons de découvrir ce langage au travers de la création de deux scripts destinés à supprimer la publicité des sites internet. Cette fonction existe sous la forme d'add-on pour Firefox mais n'est pas présente pour Internet Explorer 8 et 9. Avec nos deux scripts, la publicité disparaîtra non seulement du navigateur de Microsoft mais aussi de tous les logiciels installés. Ce filtrage pourra être désactivé pour accéder à certains contenus où le passage par la publicité est obligatoire.

Découvrez les possibilités du VBS

Le VBScript est un langage interprété : intégré au système, il n'a pas besoin d'être compilé (transformé en fichier « exécutable ») pour fonctionner. La simple extension VBS permet de rendre actif le fichier. Le résultat d'un script VBS peut apparaître dans la console ou directement dans une fenêtre Windows. Ceci dépend de l'interpréteur utilisé : CScript pour la console, WScript pour Windows. Le choix de l'interpréteur est automatique (il peut être forcé par le programmeur). Au niveau du langage en lui-même, comme

SOMMAIRE

p.56
Gérez les droits du fichier hosts
Pour filtrer la publicité, vous devrez manipuler ce fichier.

p.56
Réalisez un fichier script
Récupérez notre fichier Refreshhost.zip pour démarrer.

p.57
Pourquoi filtrer les pubs ?
Gagnez en vitesse et en sécurité lors de votre navigation sur le net.

p.58
Supprimez les pub non désirées
Testez le filtre antipub en vous rendant sur un site commercial.

p.59
VBS Factory
Ce logiciel dispose d'un débogueur pour tester vos scripts.

Release by TEAM-DZ

Pratique | Gérez les droits du fichier hosts

> LES PROPRIÉTÉS DU FICHIER HOSTS Commencez par vous rendre dans le répertoire *C:\windows\system32\drivers\etc*. Là, faites un clic droit sur le fichier *hosts* et choisissez *Propriétés*. Rendez-vous dans l'onglet *Sécurité* et cliquez sur le bouton *Modifier*.

> L'UTILISATEUR Dans la fenêtre des autorisations, cliquez sur *Ajouter* et entrez le nom de votre utilisateur. Faites *Vérifier les noms* pour qu'il corresponde au profil tel qu'il est entré dans le système. Sélectionnez l'utilisateur que vous venez d'ajouter puis, dans *Autorisations*, cochez *Contrôle total* dans la colonne *Autoriser*.

> LES AUTORISATIONS Revenez dans le répertoire *C:\Windows\System32\drivers*. Faites un clic droit sur *etc*. et choisissez *Propriétés*. Cliquez sur *Avancé* puis, dans *Propriétaire*, sur *Modifier*. Choisissez un groupe et faites *OK*. Reproduisez la même procédure que pour le fichier hosts (étape 2).

pour le VBA (Visual Basic pour les applications), on trouve la totalité des commandes dans la partie librairie du site Microsoft MSDN (http://tinyurl.com/vbscriptreference). Outre les attributs classiques des langages de programmation, VBS a accès à de très nombreux objets gérés par Windows. On peut par exemple créer des scripts pour intercepter des événements du système comme l'écriture d'un fichier dans un répertoire, interroger les éléments de surveillance du matériel ou même contrôler le navigateur Internet Explorer.
La manipulation des fenêtres est aussi une possibilité qu'offre ce langage même si, en raison de problèmes de sécurité, Microsoft a limité les possibilités d'interaction avec les applications déjà lancées par l'utilisateur. Pour écrire un programme VBScript, on peut utiliser un éditeur de texte avec coloration syntaxique. Notepad++ convient très bien. Vous pourrez le télécharger gratuitement à l'adresse http://notepad-plus-plus.org/download. On peut aussi utiliser un éditeur dédié au VBS : c'est le cas d'Astase VBS Factory.

Un éditeur bien utile : VBS Factory

VBS Factory est un éditeur spécialement conçu pour l'écriture de script en Visual Basic. Son interface assure la coloration syntaxique qui permet de bien visualiser la structure du code. Il est pourvu d'un débogueur : un environnement virtuel où peut-être exécuté le script afin de détecter les éventuelles erreurs de programmation. Le programme est aussi intéressant pour structurer de gros scripts : il détecte toutes les procédures, fonctions et classes puis les agence dans une arborescence. Vous pourrez ainsi revenir très rapidement sur un morceau de code sans avoir à chercher dans tout votre script. VBS Factory est aussi pourvu d'un assistant de création de code. Ce dernier gère l'intégration de fonctions pré-écrites comme celles qui vous permettront de connaître l'emplacement d'un fichier, son extension, de déterminer l'interpréteur à utiliser ou encore de créer un menu de choix de script à lancer. Enfin VBS Factory propose une console VBS pour tester vos commandes rapidement.
VBS Factory installe et permet d'utiliser Microsoft Script Encoder. Ce programme

Pratique | Réalisez un fichier de script

1 RÉCUPÉREZ LE SCRIPT Récupérez le fichier **http://jpbay.free.fr/refreshhost.zip** et décompressez-le à la racine de votre disque système. Lancez-le et rendez-vous dans *C:\windows\system32\drivers\etc* pour vérifier qu'un fichier hostbase.txt est bien présent.

2 CRÉEZ UNE TÂCHE PLANIFIÉE Ouvrez le menu *Démarrer* puis, dans le champ *Rechercher*, entrez *planificateur*. Ouvrez le planificateur de tâches et cliquez sur *Créer une tâche*. Donnez-lui un nom et passez à l'onglet *Déclencheurs*.

3 CRÉEZ UNE TACHE PLANIFIÉE (2) Cliquez sur *Nouveau* puis sélectionnez *Chaque semaine*, cochez un jour et indiquez un horaire qui vous convient. Ensuite, dans l'onglet *Actions*, cliquez sur *Nouveau* et pointez vers le fichier *refreshhost.vbs*.

Release by TEAM-DZ

QUESTION

Pourquoi filtrer les publicités ?

> VITESSE ET SÉCURITÉ Filtrer les sites publicitaires a deux buts : le premier est d'accélérer la vitesse de téléchargement des sites web. En effet, les contenus publicitaires ralentissent souvent l'affichage des pages. La lisibilité des sites est aussi bien plus grande sans ces éléments. La seconde raison est sécuritaire : de nombreuses régies publicitaires sont régulièrement piratées et diffusent à leur insu des malwares sur tous les sites qui affichent les bandeaux de pub. Pourquoi alors désactiver ce filtrage ? Car certains sites web imposent d'afficher les publicités pour accéder à certains contenus (M6, TF1…).

est intéressant si vous utilisez vos scripts sur d'autres ordinateurs. Il vous permettra de préserver la confidentialité de vos sources en les cryptant. VBS Factory est un programme gratuit pour une utilisation personnelle. Il est téléchargeable à l'adresse http://www.labo-microsoft.org/logiciels/11005. Pour une prise en main rapide, rendez-vous dans le menu *Fichier* de VBS Factory puis cliquez sur *Assistant nouveau VBS*. Remplissez les champs et choisissez éventuellement les fonctions à intégrer dans votre script.

Quelques règles de présentation du code

Comme pour tous les langages, l'écriture de code en VBscript obéit à certaines règles de présentation pour le rendre plus lisible : On commence par déclarer le type de chaque variable. On inscrit ensuite les valeurs qui leur seront attribuées (pour les éléments qui seront constants pendant l'exécution du code). On introduit ensuite les fonctions et on termine par le programme en lui-même. Lors de l'écriture du code, il est très important de rajouter des commentaires pour séparer les différentes étapes. Ainsi, si vous revenez sur votre programme, vous retrouverez bien plus rapidement le fonctionnement des différents éléments. C'est encore plus impératif si vous travaillez à plusieurs. Autre point très important : l'indentation. Lorsque vous utiliserez des boucles (if then, for next, while wend…), l'ajout de tabulation va vous permettre d'identifier visuellement toutes les lignes de code qui font partie de votre boucle. Dans VBS Factory, pour augmenter l'indentation de plusieurs lignes de code, sélectionnez-les et pressez les touches [Ctrl] + [i] pour décaler le code vers la droite. Pour réduire l'indentation, utilisez la combinaison de touche [Ctrl] + [h]. Si vous vous servez de notepad++, sélectionnez votre code et appuyez sur la touche [tab] pour l'indenter ou [maj]+[tab] pour réduire son indentation.

L'ASTUCE

SUPPRIMEZ LA PUBLICITÉ DE LIVE MESSENGER

Microsoft Live Messenger est un très bon logiciel de messagerie instantanée. La publicité est cependant assez présente dans son interface. S'agissant souvent de bandeaux en flash, elle vous expose aux failles de sécurité de cet élément. Pour s'en débarrasser, il suffit d'ajouter les hosts des serveurs de publicité de ce logiciel dans le fichier hostbase.txt que notre script va créer dans le répertoire *C:\Windows\system32\drivers\etc*. Éditez le fichier et ajoutez sur deux lignes *127.0.0.1 rad.msn.com* et *127.0.0.1 rad.live.com*. Relancez Live Messenger et le tour est joué : plus de publicité.

Le principe du fichier hosts : un convertisseur d'adresses

L'ensemble de scripts permettant de filtrer les sites publicitaires à la demande et sous Internet Explorer 8/9 est basé sur la manipulation d'un fichier particulier appelé « hosts ». Situé dans le répertoire *C:\windows\system32\drivers\etc*, le fichier hosts est un fichier texte auquel toutes les applications du système font appel pour traduire les adresses web en adresse IP. Ce fichier permet notamment de ne pas faire appel à un serveur DNS externe. Son fonctionnement est simple : chaque ligne doit correspondre à cette syntaxe : adresse IP suivie du hosts. Par exemple 66.249.92.104 www.google.com. Une astuce permet d'interdire aux applications d'accéder à certains sites : il suffit pour cela d'indiquer l'adresse IP « 127.0.0.1 » suivie du nom du site web. Le navigateur dans lequel sera entrée cette adresse tentera de se connecter à cette IP, qui n'est autre que celle de l'ordinateur local. C'est cette astuce que nous allons mettre à profit pour empêcher le chargement des contenus publicitaires. Il suffit pour cela d'insérer les hosts des serveurs de publicité et de les rediriger vers l'adresse 127.0.0.1. Le site www.mvps.org/winhelp2002/ propose une liste relativement exhaustive des serveurs utilisés par les annonceurs. Malheureusement, ce fichier évolue régulièrement et, pour le

4 CRÉEZ UNE TACHE PLANIFIÉE (3) Dans l'onglet *Condition*, cochez la case *Ne démarrer que si la connexion réseau suivante est disponible*. Dans le champ qui suit, choisissez *N'importe quelle connexion* pour l'ouvrir à toutes les requêtes.

5 CRÉEZ UNE TÂCHE PLANIFIÉE (4) Enfin, dans l'onglet *Paramètres*, cochez la case *Exécuter la tâche dès que possible si un démarrage planifié est manqué*. Ainsi, même si votre ordinateur n'est pas allumé à l'horaire de déclenchement, le script agira.

6 VÉRIFIEZ LE FONCTIONNEMENT Allez dans le *planificateur de tâche > Bibliothèque du planificateur*. Faites un clic droit sur la tâche que vous venez de créer et choisissez *Exécuter*. Dans le répertoire *c:\windows\system 32\drivers\etc*, le fichier hosts doit être daté du jour.

Release by TEAM-DZ

maintenir à jour, il faudrait récupérer régulièrement le document. C'est là qu'intervient notre premier VBscript. Pour réaliser un fichier de script, rien de plus simple : commencez par créer un fichier texte en cliquant du bouton droit sur le bureau puis choisissez *Nouveau* et *Document texte*. Remplacez l'extension .txt par .vbs. (voir notre astuce « Affichez l'extension de vos fichiers » page 59). Votre fichier sera alors exécuté par le gestionnaire de script. Pour éditer un fichier VBS, faites un clic droit dessus et choisissez *Edit with notepad*.

AVEC DEUX SCRIPTS VBS, **UNE LISTE DE SERVEUR ET LA MANIPULATION D'UN FICHIER,** LE WEB SE VIDE DE SA PUBLICITÉ.

Récupérez le script « refresh hosts »

Vous retrouverez notre script à l'adresse *http://jpbay.free.fr/refreshhost.zip*. Dézippez ce document pour récupérer le script. Ce dernier est doté d'une extension .txt. Vous devrez donc le renommer en .vbs pour qu'il fonctionne. Commencez par déclarer vos variables avec la commande dim. L'objet inet est créé avec *Set inet = CreateObject ("Internet Explorer.Application")*. Il s'agit tout simplement du navigateur Internet Explorer qui va vous permettre d'aller sur le site www.mvps.org/winhelp2002/hosts.txt avec la commande *inet.Navigate*. Le navigateur ne sera pas affiché (*inet.Visible = False*) pour ne pas gêner l'utilisateur. Vous allez ensuite créer un second objet qui va vous permettre de travailler avec les fichiers *Set fso = CreateObject ("Scripting.File SystemObject")*. Après avoir chargé la page web en naviguant dessus

En ajoutant le script dans le volet des favoris, il apparaît directement dans l'interface d'Internet Explorer.

(*inet.Navigate - www.mvps.org/ winhelp 2002/hosts.txt*") et attendu que la page soit chargée (*inet.ReadyState = 4*), le script récupère le contenu de la page web et le stocke dans la variable textmpvs *textmvps=inet.document.body.innerText*. Reste ensuite à intégrer ce texte dans le fichier hosts. Pour cela, on utilise dans le script l'objet fso avec les commandes *copyfile* et *openTextFile* pour copier/créer des fichiers et les ouvrir en mode texte. Notre script va d'abord sauvegarder le fichier actuel dans un document « hostbase.txt ». Il vous permettra de rajouter des hosts pour votre réseau local ou pour supprimer l'accès à des serveurs de pub qui seraient passés au travers du filtre. Si ce fichier est déjà présent, le fichier hosts actuel est copié dans host.old : *fso.copyfile "C:\Windows\System32\drivers\etc\ hosts","C:\Windows\System32\ drivers\etc\hosts.old",true*. Le script ouvre le fichier hosts. Ce dernier est stocké dans la variable *objet filehosts* avec la commande *set filehosts=fso.openTextFile ("C:\Windows\System32\drivers\etc\hosts",2)*. Ensuite, le fichier hostbase.txt est ajouté aux contenus récupérés sur le web (variable textmvps) : *With filehosts.writeline textbase & textmvps end with*. Cette écriture est dans une boucle if qui vérifie que la variable textmvps n'est pas nulle (le message « *attention impossible de récupérer www.mvps.org/winhelp2002/hosts.txt* » apparaît si c'est le cas). Attention, pour faire fonctionner le script, vous devez au préalable modifier les droits du fichier hosts (voir notre encadré pratique « Gérez les droits du fichier hosts » page 56). Mettre à jour le filtrage, c'est bien, mais pouvoir l'activer ou le désactiver à la demande, c'est mieux ! C'est l'objectif de notre second script.

Le script d'activation/désactivation

Ce script est utilisable avec Internet Explorer. Il va remplacer le contenu du fichier hosts par *hostsbase.txt*, qui est créé par le précédent script et qui contient le hosts d'origine de l'ordinateur. Ainsi, le filtrage ne s'effectuera plus sur les sites publicitaires. Une fois ce remplacement

Pratique | Supprimez la publicité non désirée

1 INTÉGREZ ADBLOCKER.VBS Commencez par décompresser le fichier **http://jpbay.free.fr/adblocker.zip**. Dans l'explorateur de fichier, rendez-vous dans le répertoire *utilisateur/nomduprofil* puis insérez le fichier *adblocker.vbs* dans *favoris/volet des favoris/*.

2 VÉRIFIEZ SON FONCTIONNEMENT Ouvrez Internet Explorer et faites un clic droit sur le bouton *Favoris*. Cochez *Volet des favoris* pour faire apparaître cette barre. Cliquez une première fois sur *adblocker*. Ceci devrait désactiver le filtrage.

3 VÉRIFIEZ SON FONCTIONNEMENT (2) Réactivez le filtrage et rendez-vous sur le site Deezer.com. Vous pourrez constater qu'entre deux morceaux, les messages publicitaires audio ont disparu. Il en va de même pour la quasi-totalité des bandeaux publicitaires.

Release by TEAM-DZ

effectué, le script va ouvrir une nouvelle fenêtre à l'intérieur d'Internet Explorer et afficher le même site puis fermer la fenêtre précédente. Cette procédure permet à Internet Explorer de recharger le hosts. Comme il n'est pas possible de prendre le contrôle d'une application déjà lancée, nous avons utilisé des raccourcis claviers (commande *Wshshell.sendkeys*). Dans le détail, le script commence par créer deux objets, wshshell et fso : *Set WshShell = WScript.CreateObject ("WScript.Shell")* et *Set fso = CreateObject ("Scripting.FileSystemObject")*. WScript.Shell est un objet qui permet notamment de contrôler les fenêtres Windows, de simuler l'entrée de touches du clavier ou encore de mettre en pause le script et d'afficher des popups. Le script vérifie ensuite la présence du fichier *hostbase.Txt* ou le crée s'il n'existe pas. (boucle *if not fso.FileExists("C:\Windows\System32\drivers\etc\hostbase.txt")*). Ensuite, le script s'assure de la présence du fichier *hostsavecmvps.txt*. Si ce fichier est là, c'est que le filtrage est désactivé. Notre programme active donc le filtre en copiant ce fichier dans *hosts* avec la commande *fso.Copyfile "C:\Windows\System32\drivers\etc\hostsavecmvps.txt","C:\Windows\System32\drivers\etc\hosts", true*. Adblock efface ensuite le fichier pour que l'exécution suivante du script effectue l'action inverse (désactivation du filtre). Pour chaque cas, le script lance la reproduction de fenêtre d'Internet Explorer avec les raccourcis [Ctrl] + [k]… *WshShell.SendKeys "^k"*. La commande *wscript.sleep(3000)* introduit un temps d'attente entre les simulations du clavier. Ces temps sont nécessaires mais vous pouvez essayer de les réduire (dans notre script, ils sont fixés à trois secondes). La boucle se termine par l'affichage d'un popup avec la commande *Wshshell.Popup "filtrage pub activé",3*.

> *Le logiciel VBS Factory dispose d'un débogueur : vous pourrez tester vos scripts VBS avant de les lancer.*

L'ASTUCE

AFFICHEZ L'EXTENSION DE VOS FICHIERS

Pour remplacer l'extension d'un fichier, elle doit s'afficher dans son intégralité. Ouvrez n'importe quel répertoire de votre ordinateur, cliquez sur *Organiser* puis choisissez *Option des dossiers et de recherche*. Dans l'onglet *Affichage*, décochez *Masquer les extensions de fichier dont le type est connu*. Terminez en cliquant sur *OK*. Ainsi, l'extension de tous les fichiers sera enfin visible. Vous pourrez alors la modifier en cliquant simplement deux fois sur le nom du fichier. N'oubliez pas d'enregistrer l'ancien et le nouveau nom du fichier pour corriger d'éventuelles erreurs ensuite.

Mettez en place les scripts et la mise à jour du host

Une fois ces deux scripts récupérés, vous devrez les intégrer dans votre système. Cette intégration s'effectue à plusieurs niveaux. Tout d'abord, il faut savoir que le fichier hosts de Windows 7 est protégé par le contrôle de compte utilisateur : il ne peut être modifié par un script sauf à lancer ce dernier en mode administrateur. Il faudra donc que l'utilisateur s'approprie ce fichier (voir notre encadré pratique « Gérez les droits du fichier hosts » page 56). Ensuite, vous allez devoir créer une tâche planifiée pour lancer le script de mise à jour du hosts. Un rythme hebdomadaire est suffisant pour récupérer le fichier proposé par le site mvps.org. Ensuite, pour que le script d'activation/désactivation fonctionne, vous devrez le copier dans les favoris du navigateur (voir notre pas à pas page 58). Enfin, lorsque vous utiliserez le script dans Internet Explorer, ne cliquez pas sur une autre application à ce moment-là : les commandes simulées par le script seraient alors transmises à cette autre fenêtre.attendez toujours l'apparition du message « *Filtrage activé/désactivé* » pour reprendre votre surf.

Jean-Philippe Bay

4 ACCÉLÉREZ LA PROCÉDURE Si vous trouvez que l'activation/désactivation du filtre est trop lente, vous pouvez adapter sa vitesse et en modifier les temps de latence WScript.Sleep(xxxx) dans le fichier adblocker.vbs. Ce temps est exprimé en millisecondes...

5 REPÉREZ LES RATÉS Certains sites d'annonceurs ne sont pas référencés dans la liste de mvps. Vous pouvez trouver leur host en faisant un clic droit sur la page web et en sélectionnant *Afficher la source*. Une recherche sur le mot « ads » donne souvent des résultats.

6 AJOUTEZ DES HOSTS Si vous trouvez de nouveaux serveurs de publicité, vous pourrez les ajouter directement dans le fichier « hostbase.txt » avec la syntaxe « 127.0.0.1 hosttrouvé » sur une nouvelle ligne de votre fichier. Relancez refreshhost.vbs pour l'intégrer à hosts.

Release by TEAM-DZ

ADMINISTREZ VOS SERVEURS À DISTANCE

Dans une TPE comme dans une grosse entreprise, **les personnes en charge du bon fonctionnement de l'informatique** doivent pouvoir intervenir à distance sur leurs serveurs. Voici différentes solutions Windows Server à mettre en œuvre.

SOMMAIRE

Small business pour les TPE
Un serveur pour accéder à n'importe quelle machine connectée à internet.

PowerShell
Doté d'un véritable éditeur visuel, il permet l'exécution de scripts évolués.

10 gadgets Windows 7
Pour administrer vos serveurs depuis votre bureau.

L'administration à distance des serveurs n'est pas simplement une fonctionnalité, c'est un devoir. Dans un monde où tous les personnels sont hypermobiles, où la frontière entre la vie personnelle et la vie professionnelle n'existe plus vraiment, où l'acquisition et le traitement des données sont intemporels et où e-mails et services web imposent une disponibilité permanente, tout administrateur, même dans une TPE avec un unique serveur SBS (Windows Small Business Server), se doit de pouvoir agir et surveiller son infrastructure à distance, n'importe quand et n'importe où. L'administration à distance revêt aussi un autre aspect : Elle consiste à contrôler son serveur (ou même ses serveurs) sans quitter son poste client et passer son temps dans la « salle des machines » face à son serveur. Mise à part des interventions matérielles, il n'existe aucune tâche qui ne puisse être réalisée à distance depuis le PC de l'administrateur.

D'autant que depuis l'origine, Windows Server a toujours mis à disposition des outils et des API pour piloter la maintenance à distance. Nous allons voir ici certains de ces outils, certaines de ces commandes, et surtout comment les mettre en œuvre.

Créez la fonctionnalité Remote Desktop

La première méthode et probablement la plus populaire pour prendre le contrôle à distance de votre serveur Windows SBS 2003/2008 (ou de toute autre version de Windows Server) consiste à mettre en œuvre la fonctionnalité « Remote Desktop » (bureau à distance), parfois plus connue sous le nom de son protocole « RDP ». Cette fonction permet d'afficher et contrôler le bureau du serveur Windows depuis n'importe quel poste Windows (et, comme on le verra plus loin, également depuis toutes sortes de terminaux). Les événements clavier et souris sur le poste local sont transmis au serveur distant ce qui permet de piloter la machine distante exactement comme si vous vous trouviez devant. Le support de cette fonctionnalité est réalisé par les « Terminal Services » de Windows Server. Ces services fonctionnent selon deux modes : Un mode « multipostes » permettant à des utilisateurs de créer des sessions virtuelles, et un mode « administration » qui est celui qui nous intéresse et qui est utilisé à des fins de gestion de l'infrastructure. Pour activer cette fonctionnalité, l'opération se révèle des plus simples : il suffit de cocher *Autoriser la connexion…* en cliquant sur *Paramètres d'utilisation à distance* dans l'outil *Système* accessible depuis le Panneau de Configuration. Notez que Windows propose en réalité deux types d'autorisation : la connexion via n'importe quelle version de RDP (moins sécurisée), ou la connexion uniquement depuis des clients RDP de dernière génération supportant NLA (Vista, Windows 7). Notez aussi que cet accès distant est automatiquement validé à tout utilisateur appartenant aux groupes Administrateurs. Si vous voulez autoriser d'autres utilisateurs ou groupe, il faudra les ajouter manuellement en utilisant le bouton *Sélectionnez des utilisateurs*. Dès lors, pour accéder à ce serveur à distance depuis n'importe quel poste, il suffit d'utiliser la dernière version du client RDP « Connexion Bureau à distance » livrée avec toutes les versions de Windows 7 (dans le menu *Accessoires*, ou saisissez *mstc* dans le champ de recherche du menu *Démarrer*) ou téléchargeable depuis le site de Microsoft pour les postes sous XP ou Vista (http://support.microsoft.com/kb/

Release by TEAM-DZ

969084). Il n'y a plus alors qu'à saisir l'adresse IP du serveur ou son nom *Netbios* pour voir s'afficher son bureau dans une fenêtre sur votre ordinateur. Tous les outils d'administration sont ainsi directement accessibles.

Définisez une stratégie de groupe…

Si votre réseau possède plusieurs serveurs Windows, il suffit de répéter la même opération sur chaque serveur puis simplement de saisir le nom ou l'adresse IP de chaque serveur dans l'outil de connexion Bureau à distance. Avec Windows Server 2008, Microsoft impose un pare-feu qui est actif par défaut sur chaque installation. Plutôt que d'aller sur chaque serveur valider l'administration distante et l'ouverture du pare-feu sur le port TCP/UDP 3389, il est préférable de définir une stratégie de groupe qui réalise cela pour vous. Pour cela, utilisez l'outil de Gestion de stratégie de groupe pour créer un nouvel « objet de stratégie » incluant les paramètres de

Les outils Sysinternals

> LES UTILITAIRES Aucun administrateur, aucun utilisateur avancé ne peut ignorer la collection d'utilitaires de Sysinternals, autrefois société indépendante d'outils système et désormais incorporée au giron Microsoft. Le site live.sysinternals.com comporte quelques outils indispensables au quotidien, comme Autoruns (contrôle des zones en autoexécution) ou Process Explorer (un outil de chasse aux bugs et codes malveillants en mémoire). Cette collection contient aussi quelques outils très utiles pour piloter à distance vos serveurs et souvent désignés sous le nom de « PS Tools ». Parmi ceux-ci, on retiendra particulièrement :

PsExec qui permet de lancer à distance l'exécution d'une commande ou d'un programme.

PsList liste à distance les processus en cours d'exécution sur le serveur.

PsKill tue à distance un processus ou un programme en cours d'exécution sur le serveur.

PsFile relève à distance les fichiers ouverts sur le serveur.

PsLoggedOn permet de vérifier à distance qui est logué sur le serveur.

PsShutdown redémarre à distance le serveur.

PsInfo délivre toutes sortes d'informations plus ou moins utiles sur le serveur, notamment sa durée de fonctionnement depuis le dernier redémarrage.

Ne perdez pas de vue que toutes ces commandes sont des lames à double tranchant. Laissées entre les mains de gens mal intentionnés, elles peuvent se révéler redoutables. Et même s'il faut préciser un nom d'utilisateur et un mot de passe, n'oubliez jamais que ces informations sont véhiculées en clair à travers le réseau avec ces outils.

Pas à pas | Installez un Remote Desktop et prenez le contrôle du serveur

1 INSTALLATION Ouvrez le menu *Démarrer* de Windows Server 2008, cliquez du bouton droit sur *Ordinateur* et choisissez *Propriétés*. Cliquez sur *Paramètres d'utilisation à distance*. Cochez *N'autorisez que la connexion des ordinateurs exécutant Bureau à distance avec authentification*.

2 VALIDATION Ouvrez le menu *Démarrer*, saisissez *pare-feu* et lancez le Pare-feu avec *Paramètres avancés*. Sélectionnez *Règles de trafic entrant*. Triez la liste par ordre alphabétique et assurez-vous que la case *Bureau à distance* est bien cochée.

3 UTILISATION Allez sur votre poste Windows 7. Ouvrez le menu *Démarrer* et saisissez *Bureau* puis cliquez sur *Connexion Bureau à distance*. Saisissez l'adresse IP de votre serveur et cliquez sur *Connexion*. Le bureau du serveur apparaît dans une fenêtre.

Release by TEAM-DZ

LOGICIEL...

Pour compléter les fonctionnalités standards d'administration de Windows Server, découvrez un étonnant logiciel d'administration, fruit des communautés open source. HealthMonitor est un outil de surveillance système gratuit. Fonctionnant en tâche de fond sous forme de service NT, il analyse et vérifie l'état de fonctionnement du serveur (ou de n'importe quel PC) puis notifie l'administrateur par e-mail ou SMS dès qu'une alerte est détectée...

http://sourceforge.net/projects/healthmonitor

sécurité suivants (présents dans l'arborescence Pare-feu Windows avec fonctions avancées -> Règles de trafic entrant) : administration à distance (RPC-EPMAP), administration à distance (NP-Entrée) et administration à distance (RPC). Ces trois règles permettent d'autoriser tous les services d'administration à distance dans le pare-feu et ne s'appliquent pas qu'à RDP.
Si vous devez contrôler plusieurs serveurs depuis votre poste de travail, il est souvent préférable d'utiliser la version du client RDP intégrée à la MMC (Microsoft Management Console, la console d'administration présente dans Windows Server et dans les éditions Pro de Windows). Avant cela, il vous faudra installer cette fonctionnalité Windows qui appartient au kit RSAT (voir plus loin) que vous devrez avoir préalablement mis en place. Ouvrez le menu *Démarrer*, saisissez *fonctionnalités* dans champ de recherche et cliquez sur *Programmes et fonctionnalités*. Cliquez sur *Activer ou Désactiver des fonctionnalités Windows*. Dans la liste des fonctionnalités, repérez l'arborescence Outils d'administration de serveur distant et déployez-la. Affichez Outils d'administration des rôles. Cochez la case *Outils des services Bureau à distance*. Ouvrez le menu *Démarrer* de Windows 7, et saisissez *tsmmc.msc* dans le menu de recherche puis validez avec *Entrée*. Vous pourrez ainsi enregistrer et gérer plus facilement tous vos serveurs au travers de cette application multifenêtre.

Serveur | Small Business Server 2011 Essentials

Remote Web Access Microsoft a introduit un nouveau serveur à l'intention des TPE de moins de 25 employés. Dénommé Windows Small Business Server Essentials, ce serveur propose notamment une fonctionnalité simple à installer et à paramétrer pour permettre aux administrateurs, comme aux autres utilisateurs, d'accéder en toute sécurité à leur propre PC, mais aussi à leurs fichiers et cela depuis n'importe quelle machine connectée à internet grâce à une interface web. Aucune compétence informatique n'est nécessaire, il suffit d'ouvrir un navigateur web pour accéder à un miniportail d'entreprises qui propose d'accéder très facilement aux dossiers de l'utilisateur et aux dossiers partagés. L'utilisateur peut alors récupérer ou envoyer des fichiers vers les espaces de stockage. Il peut également accéder à distance à l'écran de son ordinateur professionnel (s'il l'a laissé allumé). Ce minisite web peut être étendu au travers de gadgets et add-in afin d'y ajouter des fonctionnalités d'informations, de calendriers, de forums, ou même de travail collaboratif. Un vrai plus pour votre TPE.

Configurez un accès VPN sur le poste qui accède au réseau

Pouvoir ainsi piloter l'écran de ses serveurs sans être physiquement présent devant eux constitue un gain de temps et d'efficacité remarquable. Jusqu'ici nous avions administré les serveurs depuis un poste du réseau local. Mais il serait bien plus utile de pouvoir les administrer via internet. La solution la plus simple, et la plus accessible à tous, consiste à ouvrir un accès VPN (Virtual Private Network) qui permet aux utilisateurs autorisés de connecter n'importe quel PC au réseau local à travers internet. Pour des raisons de sécurité, veillez à n'autoriser cet accès qu'à vous seul, si possible au travers d'un login spécifique aux droits astucieusement choisis et au mot de passe très fort et fréquemment modifié. L'ouverture d'un VPN est une opération triviale, notamment sous Windows SBS 2008. Il suffit de lancer la console SBS, d'aller dans la section *Réseau* puis dans l'onglet *Connectivité* et de suivre l'assistant « Pas à pas » qui se cache derrière le lien *Configurer un réseau privé virtuel*. Il reste une dernière étape : paramétrer le pare-feu de la box ou du routeur qui connecte votre entreprise à internet. Deux solutions

Pas à pas | Installez un VPN pour accéder au réseau en toute sécurité

1 DYNDNS L'assistant *Se connecter à Internet* de Windows SBS 2008 se charge de vous attribuer un nom de domaine associé à un mécanisme DynDNS de prise en charge de l'allocation d'une IP dynamique par votre FAI. Il suffit de le suivre.

2 PARE-FEU Si votre routeur/box n'est pas compatible UPnP, vous devrez vous-même paramétrer un transfert de port (Port Forwarding) du port TCP 1723 vers l'adresse IP de votre serveur SBS 2008, via l'interface utilisateur de votre box/routeur.

3 ACCÈS VPN Depuis chez vous, sur votre ordinateur Windows 7 connecté à internet, saisissez *VPN* dans le menu *Démarrer* et cliquez sur *Configurer une connexion réseau privé virtuel*. Saisissez alors l'adresse externe du serveur ou son URL DynDNS.

Release by TEAM-DZ

sont possibles : soit activer le mode UPnP de votre routeur (dans ce cas, SBS devrait pouvoir configurer automatiquement le pare-feu), soit réaliser manuellement un « Port Forwarding » (Transfert de port) du port TCP 1723 vers l'adresse IP interne du serveur (l'opération varie d'un routeur à l'autre ou d'une box à l'autre, reportez-vous aux manuels). À noter que pour pouvoir ainsi accéder à distance à son réseau et ses serveurs, il faut connaître l'adresse IP externe de votre entreprise. Si votre FAI ne vous en fournit pas une fixe mais vous en attribue une dynamiquement, vous pourrez soit utiliser la fonction DynDNS de votre box/routeur, soit exploiter l'assistant Gestion de votre adresse internet de SBS 2008, qui vous permet d'obtenir un nom de domaine auprès de trois fournisseurs habilités à délivrer à SBS un service DynDNS sans autre paramétrage de votre part. La dernière opération consiste à configurer cet accès VPN sur le poste qui doit accéder au réseau (par exemple le PC de votre domicile). Sous Windows 7, ouvrez le menu *Démarrer*, saisissez *VPN* dans le champ de recherches et sélectionnez *Configurer une connexion réseau privé virtuel*. Il suffit alors de saisir l'adresse IP fixe de votre entreprise, ou le nom de domaine associé à votre DynDNS.

Accédez aux outils d'administration classiques…

Mais la prise de contrôle à distance du bureau des serveurs est loin d'être l'unique moyen d'administrer des serveurs. En réalité, la plupart des composants enfichables (Snap-in) de la MMC ainsi que certaines applications classiques comme « Regedit » permettent de se connecter à distance à un serveur. La MMC vous permettra notamment d'accéder directement aux outils d'administration classiques des serveurs que sont l'Observateur d'événements, le Gestionnaire de serveur, le Gestionnaire de périphérique, la Gestion des disques et les snap-in comme Services, Dossiers partagés, Utilisateurs et groupes locaux. Dans tous les cas, il suffit de lancer la MMC (tapez *MMC* dans le menu *Démarrer*), d'aller dans *Ajouter/supprimer un composant logiciel enfichable*, de choisir un composant (par exemple *Gestion de l'ordinateur*), de cliquer sur *Ajouter*, de sélectionner *Un autre ordinateur* et de donner le nom ou l'adresse IP du serveur. Comme nous le verrons plus loin, il existe un moyen plus pratique d'accéder à toutes ces fonctionnalités au travers de l'outil RSAT.

Pratique | Contrôlez vos serveurs en quatre étapes

1 BUREAUX MULTIPLES Une fois le kit RSAT installé et téléchargé, vous pouvez librement administrer tous vos serveurs à distance. L'outil *Bureaux à distance* permet de contrôler plusieurs serveurs depuis une seule et même fenêtre MMC.

2 ANALYSE DES JOURNAUX Via l'observateur d'événements, vous pouvez vous connecter à chacun de vos serveurs, repérer les anomalies et les alertes présentes dans les journaux de sécurité, des applications et du système, et contrôler que tout fonctionne normalement.

3 DOSSIERS PARTAGÉS Parmi les modules d'administration de RSAT, le gestionnaire de dossiers partagés s'avère très pratique au quotidien. Il permet d'ajuster les droits et de créer sur tous vos serveurs de nouveaux espaces de stockages partagés en quelques clics.

4 POSTE DE PILOTAGE Utilisez la MMC et ses composants enfichables pour créer votre poste de pilotage personnalisé pour tous vos serveurs. Vous pourrez ainsi administrer l'ensemble de vos serveurs en toute convivialité et sécurité depuis votre poste de travail sous Windows 7.

> LA PLUPART DU TEMPS, LES ADMINISTRATEURS SE CONTENTENT **DE PIOCHER DANS LA GIGANTESQUE BASE DE SCRIPTS PRÉDÉFINIS** FOURNIE PAR TECHNET…

Piochez dans la base de scripts fournie par Technet

Depuis quelques années, Microsoft a introduit au cœur de Windows un framework d'administration connu sous le nom de WMI (Windows Management Instrumentation). Via WMI on peut presque tout connaître des ordinateurs et serveurs connectés au réseau local, ainsi que sur le domaine et ses utilisateurs. En général, on utilise WMI au travers de scripts VBScript. Connaître toute la richesse de WMI nécessite d'y consacrer un temps important. La plupart du temps, les administrateurs se contentent de piocher dans la gigantesque base de scripts prédéfinis fournie par Technet et de la personnaliser selon leurs besoins. Pour en savoir davantage sur WMI et tout ce qu'on peut faire avec, mais aussi pour télécharger des scripts prêts à l'emploi, connectez-vous sur l'URL : www.microsoft.com/technet/scriptcenter/

Release by TEAM-DZ

WMI est plus adapté à une administration en réseau local. Basé sur l'infrastructure DCOM (Distributed COM), WMI nécessite d'ouvrir le port 135 sur les pare-feux. Mais ce serait une grave erreur de sécurité que d'autoriser un tel accès depuis l'extérieur.

L'outil RSAT : un kit d'administration gratuit

RSAT, acronyme de « Remote Server Administration Tools », disponible en versions 32 et 64 bits pour Windows 7 regroupe tous les outils nécessaires à l'administration des rôles et fonctionnalités des serveurs Windows Server 2008, y compris l'administration des services de la déclinaison « Windows Server Core ». En fait, l'ensemble reprend nombre de snap-in MMC déjà évoqués plus haut mais en ajoute aussi de nouveaux. RSAT est un kit d'administration gratuit et librement téléchargeable depuis : http://bit.ly/cDqFu1. Une fois le logiciel installé, vous découvrirez que le menu Outils d'administration de votre Windows 7 s'est considérablement enrichi, tout comme la liste des « composants logiciels enfichables » disponibles depuis la MMC. RSAT permet ainsi d'accéder depuis la MMC de son poste Windows 7 aux mêmes fonctionnalités que la MMC de vos serveurs…

La surveillance par e-mail de votre réseau

L'administration d'un réseau consiste également à en surveiller quotidiennement le bon fonctionnement. Ceux qui ont opté pour Windows SBS 2008 disposent de fonctions de reporting très utiles, qu'ils peuvent se faire envoyer automatiquement par e-mail chaque jour. Ainsi, tous les matins au réveil, vous pouvez obtenir sur votre BlackBerry, par exemple, un récapitulatif de l'état de santé des serveurs, de l'occupation des disques, des incidents de sécurité et du bon fonctionnement des sauvegardes nocturnes. Par défaut, SBS 2008 produit deux rapports (le rapport résumé et le rapport détaillé), mais vous pouvez personnaliser ces rapports et définir précisément les rubriques et éléments que vous voulez y voir figurer. Les rapports comportent six rubriques : sécurité (statut des antivirus et pare-feux du réseau), mises à jour (y a-t-il des mises à jour en cours ou en échec), sauvegarde (état et éventuelles erreurs des différentes sauvegardes), alertes, messagerie (utilisation d'Exchange, taille des bases, nombre d'e-mails échangés) ainsi que la liste des événements critiques présents dans les journaux. Ces rapports, leur fréquence d'envoi ainsi que l'e-mail destinataire, se configurent depuis la section Rapport de la console SBS.

Accédez à vos serveurs grâce à votre iPad

Pour terminer, de même qu'il est aujourd'hui possible de recevoir des rapports sur n'importe quel périphérique et mobile grâce aux e-mails, il est aussi possible d'intervenir sur ses serveurs et de les surveiller depuis n'importe quel périphérique via RDP. Il n'y a donc pas que les ordinateurs qui sont utilisables pour administrer les serveurs. Microsoft distribue ainsi gratuitement une version de son client RDP pour les postes Mac sous OS X (elle est disponible ici : www.microsoft.com/mac/remote-desktop-client). En attendant la disponibilité de véritables tablettes Windows, on peut aussi utiliser son iPad pour accéder à ses serveurs où que l'on soit dans l'entreprise. Plusieurs clients RDP sont en effet disponibles sur la tablette Apple, dont Desktop Connect d'Antacea ou Remote Desktop Lite de Mocha. Bien que l'écran soit moins adapté, vous pouvez aussi espérer intervenir sur les serveurs depuis votre BlackBerry (www.rmdplus.com) ou votre iPhone (www.mochasoft.dk). **Loïc Duval**

PowerShell | L'administration via les scripts

Conservez vos originaux **Issue du DOS et présente depuis l'origine des temps informatiques, l'invite de commandes et ses fameux « .BAT » paraît aujourd'hui bien archaïque et limitée. Depuis Vista et Windows 2008, Microsoft, lui, a trouvé un « super » remplaçant : PowerShell. Désormais doté d'un véritable éditeur visuel, PowerShell permet l'exécution de scripts évolués basés sur un langage de programmation objet. Il permet non seulement de contrôler tous les aspects du système, mais également de contrôler tous les rôles Windows et tous les serveurs Microsoft tels que SharePoint, SQL Server et Exchange. Dès lors, il devient possible d'automatiser les tâches d'administration les plus complexes. Avec PowerShell 2.0, vous pouvez désormais exécuter ces tâches à distance. Pour vous aider dans vos premiers pas, il existe un générateur automatique de scripts WMI : PowerShell Scriptomatic. Il est téléchargeable à l'adresse : http://technet.microsoft.com/en-us/library/ff730935.aspx**

L'ASTUCE

Abracadabra Sous Windows Server 2003, les administrateurs utilisaient souvent la commande *mstsc.exe /console* pour se connecter à la session administrateur de la console physique (la session 0). Sous Windows Server 2008, la session 0 est réservée aux services. On utilise à la place la commande *mtsc.exe /admin*.

À SAVOIR… Remote Web Workplace

> LA RÉFÉRENCE… Comment offrir aux utilisateurs un accès à distance à leurs e-mails et à leur poste de travail? Si l'entreprise a opté pour un serveur SBS 2008, une telle fonctionnalité est disponible en standard et même totalement préparamétrée pour vous lors de l'installation automatisée du serveur. Dénommée RWW (Remote Web Workplace), cette fonction présente aux utilisateurs un site web dynamique, qui sert de point d'entrée unique et sécurisé vers le réseau de l'entreprise sans mettre en œuvre de VPN. Depuis ce portail, les collaborateurs nomades ont accès depuis n'importe quel navigateur web à leurs e-mails, tâches et calendriers (accès Outlook Web Access), au site SharePoint de l'entreprise et même à leur ordinateur via une connexion bureau à distance affichée sous le navigateur. Ce même espace permet aussi à l'administrateur de prendre le contrôle à distance du serveur. RWW évite d'avoir à gérer un VPN et simplifie la mise en œuvre d'une administration depuis la Toile. La solution constitue donc une alternative aux fonctions d'administration classiques. Elle présente des avantages (simplicité d'emploi, accès externe) mais aussi des inconvénients, notamment lorsqu'on est dans les murs de l'entreprise (elle reste avant tout une solution d'accès externe).

Release by TEAM-DZ

À découvrir | Six alternatives pour administrer votre réseau

> IntelliAdmin Network Administrator d'IntelliAdmin

Cet utilitaire vous permet d'effectuer des réglages, modifications et mises à jour à travers le réseau. Il peut ainsi reconfigurer les paramètres de passerelle ou les paramètres DNS et DHCP de tous vos postes. Il sait remettre à jour les horloges de tous vos serveurs et de tous vos postes. Il permet de contrôler les services à distance et d'activer ou désactiver certains services à travers tout le réseau, ce qui s'avère très utile en cas d'attaque « zero-day » sur l'une des composantes de Windows. Il peut également reconfigurer tous les postes pour forcer certains paramètres Office. Plus étonnant encore, il peut tuer un processus défini par son nom sur toutes les machines connectées au réseau et même activer la prise de contrôle à distance sur les serveurs ou postes mal configurés.

Prix 150 € environ + version d'essai disponible
www.intelliadmin.com

> DameWare NT Utilities v6 de DameWare

DameWare NT Utilities est l'un des toolkits Windows les plus réputés du marché. Il permet de s'affranchir de bien des limites de la MMC (Microsoft Management Console) pour gérer à distance vos serveurs et vos stations de travail Windows. Il simplifie les opérations sur l'Active Directory en offrant toutes sortes de fonctions de recherche et de filtrage, et permet la mise à jour simultanée de multiples objets ou attributs (comme les photos des employés, etc.). Ce toolkit comporte également un système de prise de contrôle sécurisé (Mini Remote Control) et l'outil DW Exporter qui permet d'exporter un rapport (et d'obtenir une vue graphique) de toutes les informations réseau (ordinateurs, groupes, disques, partages, utilisateurs, etc.). À essayer d'urgence.

Prix 250 € environ + version d'essai 30 jours
www.dameware.com

> Radmin 3.4 de Famatech

Radmin est l'une des plus anciennes et des plus connues solutions de prise de contrôle à distance de PC, réputé pour sa fiabilité et surtout sa rapidité même en cas de bande passante étroite (ça marche même avec une simple connexion GPRS !). Il est aussi connu pour sa sécurité puisque le logiciel prend en charge Active Directory et Kerberos tout en proposant sa propre méthode d'authentification sur 2 048 bits ! Il est bien adapté au support de multiples utilisateurs, grâce à ses fonctions de chat vocal et de chat textuel « multiuser », et son mode permettant les connexions multiples simultanées possède même un écran distant pour inviter vos collègues à une présentation ou une formation à partir de votre propre écran d'ordinateur. Un produit au potentiel très varié.

Prix 38 € environ + version d'essai 30 jours
www.radmin.fr

> Hyena 8.5 de SystemTools

Gestion des serveurs et des utilisateurs, contrôle et surveillance des services, manipulations sur l'Active Directory, gestion des événements, administration des disques et des fichiers, fonctions de reporting et d'inventaire, Hyena est un toolkit pour administrateurs avertis parmi les plus complets du marché. Pas étonnant dès lors qu'il soit aussi l'un des plus populaires du monde Windows. Il propose des fonctions d'analyse des failles de sécurité et des espaces disques, de changement des mots de passe des comptes d'administration, de centralisation et de planification des tâches d'administration du réseau. Il intègre également des fonctions de prise de contrôle à distance basées sur VNC.

Prix 145 € environ + version d'essai 30 jours
www.systemtools.com

> Spiceworks IT Desktop 5.0 de Spiweworks

Voici l'une des trousses à outils les plus complètes du marché. À la fois outil d'inventaire, de gestion et de supervision, ce logiciel sait explorer le réseau et y découvrir tous les PC, Macs, Linux et autres serveurs, routeurs ou imprimantes qui y sont connectés et en affiche leurs caractéristiques techniques. Il en fait de même avec le parc logiciel. Ces puissantes fonctions d'analyse et de supervision permettent de détecter et diagnostiquer toutes sortes de problèmes sur le réseau, y compris les manques d'espace disque, les antivirus désactivés ou non à jour, les pannes serveurs, les niveaux d'encre des imprimantes, les saturations de bande passante, les temps de réponse des bases SQL Server. Il propose de nombreux rapports prédéfinis.

Prix Gratuit !
www.spiceworks.com

> Solutions LogMeIn

Difficile d'évoquer des solutions de prise de contrôle à distance sans aborder les multiples solutions proposées par LogMeIn, l'un des leaders en la matière. Son offre est particulièrement riche couvrant les besoins ponctuels et gratuits (LogMeIn Express), aux problématiques de connectivité par réseau privé sécurisé (LogMeIn Hamachi) et d'automatisation de l'administration de parcs informatiques (LogMeIn Central), en passant par l'assistance à distance via internet sans installation logicielle préalable (LogMeIn Rescue). La grande force de LogMeIn réside dans la compatibilité de ses solutions avec les navigateurs web ainsi qu'avec une panoplie exhaustive de smartphones. Avec ces solutions, on peut assurer le support des utilisateurs de smartphones !

Prix Dépend des outils
www.logmein.com

Release by TEAM-DZ

10 GADGETS WINDOWS 7 GRATUITS pour gérer vos serveurs depuis votre bureau !

> W-SRVMON
Il permet de garder un œil sur un ou plusieurs serveurs distants et d'en superviser les principaux services. Idéal pour vérifier qu'Exchange, SQL Server ou le DHCP ne sont pas tombés en panne. http://bit.ly/cnRVuS

> REMOTECONNECT
Permet de lancer des prises de contrôle à distance selon différents protocoles. Il supporte RDP, mais aussi Telnet, VNC ou PuTTY. Pratique notamment si vous avez aussi des serveurs ou appliances Linux. http://bit.ly/ck8wAv

> RDP QUICKLAUNCHER V1.2
Moins convivial, mais plus compact et plus immédiat que Remote Desktop, RDP Quicklauncher est là encore un gadget bien pratique pour accéder plus rapidement à la prise de contrôle à distance de vos différents serveurs. http://bit.ly/9t3sQt

> SYSTEM MONITOR
Cet accessoire affiche les performances de votre PC, son adresse IP interne et externe, la quantité de mémoire disponible, et possède quelques outils réseaux toujours pratiques au quotidien. http://bit.ly/564TFh

> SERVER PING
Il permet de surveiller la disponibilité de plusieurs serveurs. La version gratuite supporte jusqu'à 5 serveurs web. La version Pro en supervise 25. Le gadget indique également leurs temps de réponse. http://bit.ly/b6tdZD

> NETWORK MONITOR II
Le logiciel supervise votre connexion internet vous rappelant votre adresse IP externe, le taux d'utilisation du réseau, les débits montants et descendants et différentes autres données. http://bit.ly/dinngs

> REMOTE DESKTOP
Ce gadget facilite la connexion à distance à différentes machines via RDP ou XenApp. Toutes deviennent disponibles en un clic depuis le bureau, ce qui s'avère très pratique surtout si l'on doit administrer plusieurs serveurs sur le réseau. http://bit.ly/cH7CMk

> SQL LAUNCHER GADGET
Ce gadget vous permet d'appeler la console d'administration de SQL Server (SQL Management Studio) avec une connexion directe à la base de données indiquée. L'idée reste donc d'utiliser plusieurs instances du gadget; une par base à administrer. http://bit.ly/bgB7oD

> RUNCOMMAND
Minimaliste, c'est l'équivalent de la commande [Windows] + [R] en version plus accessible. Avec lui, vous pouvez lancer n'importe quelle commande ou application depuis le bureau. http://bit.ly/99a6LK

> FAB-SQL SERVER SERVICES CONTROLER
Sur le papier, ce gadget permet d'activer ou désactiver vos serveurs SQL. En réalité, il exécute des batchs SQL que vous pouvez facilement personnaliser pour réaliser à distance toutes sortes d'opérations SQL Server. http://bit.ly/bJfx4R

Release by TEAM-DZ

Créez la clé USB de la dernière chance

Même lorsque le système refuse de démarrer **après une attaque de virus, il est encore possible de tenter une désinfection.** Il faut pour cela disposer d'une clé USB contenant à la fois un système autonome de secours et un antivirus.

NIVEAU

Intermédiaire

MATÉRIEL NÉCESSAIRE

- PC sous Windows 7/Vista/XP
- Clé USB 2.0 capacité 1 Go
- Unetbootin 4.x
- Avira Rescue Rescue System
- Connexion à internet

TEMPS DE RÉALISATION

30 à 40 minutes

Avec les antivirus, contre-espions, antihameçons, l'utilisation quotidienne d'un PC se déroule sous haute sécurité. Surtout depuis que le Centre de surveillance disponible avec Windows Vista, puis Windows 7, signale à l'utilisateur tout dispositif de surveillance manquant à l'appel. Si l'on ajoute à ce centre les pare-feux, les translateurs d'adresses IP et autres filtres de contenus, Windows finit par ressembler à un camp retranché. Cet empilement d'auxiliaires de sécurité suscite deux remarques. D'abord, une telle surenchère de défense dévore la puissance disponible et la sécurité ainsi apportée reste fragile. La principale cause de débordement desdites défenses est l'absence de mise à jour de la base des signatures de virus, chevaux de Troie, etc. liée à une licence devenue obsolète ; un défaut auquel les antivirus gratuits sont moins exposés. Les risques que survienne une infection en dépit de toutes les protections sont malheureusement bien réels. Pour y faire face, il faut une arme secrète pouvant être utilisée même lorsque le système ne démarre plus. À cette fin, nous allons installer un système de sauvetage, basé sur Avira Antivir, sur un CD-ROM ou mieux, sur une clé USB qui permettra de démarrer la quasi totalité des PC actuels et de les réparer à la volée.

1 Récupérez des fichiers « prêts à graver »

La première étape consiste à télécharger les fichiers permettant de disposer d'un système de sécurité totalement indépendant du système installé sur l'ordinateur infecté. Vous devez disposer d'une connexion à internet rapide, car l'une ou l'autre version du fichier pèse environ 220 Mo. Pour trouver la dédinaison de l'antivirus Avira Antivir qui nous intéresse, rendez-vous sur www.avira.com/en/support et choisissez la sous-rubrique *Download*. Dans la section *Support Tool Download*, diquez sur le lien *Avira Antivir Rescue System*. Page suivante, deux versions sont proposées : la première se présente sous la forme d'un fichier exécutable, la seconde sous la forme d'une archive au format ISO (.iso). Fonctionnant sous Windows, la déclinaison exécutable permet de graver un CD bootable sans faire appel à un programme extérieur. La seconde est celle qui nous intéresse pour travailler à partir d'une clé USB.

2 Créez la clé USB de désinfection

Une fois en possession de l'archive au format .iso, transférez son contenu sur une clé USB que le programme UNetbootin va rendre bootable. Première étape, sélectionnez la clé USB qui va servir de cible, sauvegardez éventuellement ce

L'INDISPENSABLE UNETBOOTIN

L'utilitaire UNetbootin (unetbootin.sourceforge.net) permet d'installer sur une clé USB l'image (.iso) d'un système ou d'une ressource logicielle conçue pour être gravée sur CD ou DVD.

1

2

Release by TEAM-DZ

L'ASTUCE : DES OUTILS PRÊTS À INSTALLER

Il existe déjà deux antivirus autonomes s'exécutant à partir d'un système Linux allégé : Avira Antivir et Kaspersky Antivirus. Il est possible d'essayer ce dernier en l'installant directement depuis internet via UNetbootin. Ce programme permet de sélectionner des outils Linux complets. Au milieu de cet inventaire à la Prévert, on remarquera Parted Magic, un logiciel autonome permettant de réparer les partitions endommagées et de régénérer le secteur de démarrage.

qu'elle contient puis formatez-la – le standard FAT32 conviendra – pour disposer d'un support vierge. Lancez ensuite le programme UNetbootin puis diquez sur la case de sélection *DisqueImage*. À l'aide du bouton situé en bout de ligne, parcourez l'arborescence pour accéder au dossier où est enregistré le fichier *rescue_system_common_en.iso*. Sélectionnez ensuite la clé USB qui a été précédemment préparée en vous servant du sélecteur déroulant situé au bas de la fenêtre. Lancez l'opération en appuyant sur *OK* et le transfert des fichiers commence immédiatement (prévoir de 30 s à environ 3 mn en fonction de la vitesse de la clé).

3 Démarrez l'ordinateur à partir de la clé USB

Sur PC, il existe deux stratégies pour choisir l'unité de démarrage. La plus classique consiste à visiter le BIOS (Basic Input-Output System) de l'ordinateur et à changer l'ordre des unités supportées par la séquence de démarrage. Sans en passer par là, de nombreux PC permettent d'afficher un menu de sélection au lancement (généralement via la touche de fonction [F11] ou [F12] et à condition d'être rapide). Une fois que la dé USB préparée précédemment est devenue l'unité principale, un écran monochrome apparaît. Appuyez sur la touche [Entrée] pour lancer le chargement du système Linux allégé servant de socle à notre outil de réparation d'urgence. La première opération effectuée par ce dernier consiste à transférer en mémoire la base de données virales.

4 Mise à jour et configuration de l'outil

Le système de récupération se comporte comme un programme antivirus des plus classiques. Dans l'angle supérieur droit, une liste déroulante fait apparaître une dizaine de choix de langues. Sélectionnez le français pour mieux maîtriser l'interface et les fonctionnalités. La première opération consiste à mettre la base des signatures virales à jour. Pour cela, il faut évidemment que l'ordinateur soit relié à internet (c'est au cours du chargement que le système repère le support de connexion). Il faut privilégier une connexion filaire, via le port ethernet du PC. Dans le cas où la connexion n'est pas détectée, l'opération échoue. Il reste possible d'effectuer la mise à jour en vous servant d'un autre ordinateur, soit en démarrant la clé sur ce dernier, soit en générant une nouvelle clé à partir d'un fichier nouvellement téléchargé.

5 Réglez des paramètres de recherche des virus

L'onglet *Configuration* du système intégré de détection virale est un passage obligé. Il faut à cette étape s'assurer que la réparation des fichiers est activée. Cette option peut donner de bons résultats avec les infections connues et permettre de récupérer un système fonctionnel. Par contre, il est indispensable de ne pas détruire les fichiers lorsque la réparation est impossible. Les renommer suffira pour tenter une restauration plus fine si nécessaire. Il est évidemment préférable d'ausculter tous les fichiers même si cette approche est plus lente. Il est intéressant de cocher les six premiers dangers étendus mais quasi inutile d'inclure les programmes de compression.

6 Dernière étape : lâchez les chiens

Rendez-vous sur le premier onglet pour lancer la détection des virus. Avant cela, vous pouvez encore ajouter de nouvelles unités de stockage de données en allant sur l'onglet intitulé *Autres* pour diquer sur l'option *Intégrer tous les appareils*. S'exécutant à partir d'un système dont les fonctionnalités sont limitées, le scanner de virus travaille avec une vitesse plus élevée que s'il s'exécutait sous Windows. Il ne faut que quelques minutes pour balayer un volume de plusieurs gigaoctets. Lorsqu'un virus est détecté, un message d'alerte s'affiche à l'écran et une tentative de désinfection est lancée. Le fonctionnement à partir d'une unité indépendante interdit, en revanche, le placement des fichiers en quarantaine. À l'issue de l'opération, vous pourrez tenter de lancer normalement le système désinfecté après avoir retiré la clé USB. **Thierry Pigot**

Release by TEAM-DZ

Détectez l'activité d'un bot depuis le réseau

Dès lors qu'un logiciel malveillant a pris le contrôle d'un ordinateur, **il peut devenir presque impossible de le détecter depuis le système local.** Il est plus facile de surveiller une éventuelle activité malveillante depuis une autre machine sur le réseau.

NIVEAU

Expert

MATÉRIEL NÉCESSAIRE

- Deux PC, un hub ou deux cartes ethernet.

TEMPS DE RÉALISATION

90 minutes

Les virus actuels sont des logiciels très sophistiqués et parfois capables d'échapper à un examen approfondi. À la faveur d'une faille du système non corrigée à temps, ils installent généralement un espion de clavier, un relais de spam ou un logiciel d'attaque distribuée. Le tout est commandé à distance et loué à l'heure par des mafias bien organisées. Or ces programmes peuvent passer inaperçus. Comment font-ils ? Constamment, ils se mettent à jour et changent de forme. Ainsi, l'explorateur de tâches et même les commandes DOS ne révèlent rien des intrus. Il est très difficile, même pour un spécialiste, de montrer la présence d'un rootkit depuis la machine qui l'héberge. Les logiciels antirootkits ne sont pas infaillibles. L'espoir, c'est qu'il est possible de détecter un bot par l'activité qu'il génère sur le réseau. Même s'il n'est pas actif en permanence, un bot doit se synchroniser avec son botnet. Les connexions qu'il initie peuvent être interceptées, filtrées et analysées depuis une autre machine connectée au même réseau local.

1 Installez un autre ordinateur Le poste d'observation est donc un autre ordinateur dont on peut être sûr. On commence par y installer un nouveau système, sans oublier les mises à jour de sécurité. Peu importe le système car Wireshark, le logiciel d'analyse du réseau que vous allez employer, fonctionne sur Windows, Mac OS, Linux. Téléchargez le logiciel sur Wireshark.org (Windows/MacOS) ou installez-le à partir du système de paquetage propre à la distribution Linux, si vous êtes dans ce cas. Suivant la configuration du réseau, cette machine aura besoin d'une ou deux interfaces réseau, Wi-Fi ou ethernet. Dans la suite de l'article, nous appellerons cet ordinateur « la sonde ».

2 Configurez le réseau local L'essentiel est que la sonde, la machine où est installé Wireshark, puisse voir ce que le PC suspect échange avec la passerelle vers internet (le routeur, la box). Les paquets émis entreront par les interfaces réseau de la sonde. Dans le cas du Wi-Fi, il n'y a rien de plus à faire qu'à joindre la sonde au réseau sans fil. Elle pourra alors capter tous les paquets émis par toutes les machines connectées à ce réseau. Pour une connexion filaire, par ethernet, c'est un peu plus compliqué. Vous devez d'abord vous assurer que la box est configurée en mode routeur et non en pont, parce qu'il faut connecter plusieurs machines en même temps. Ces dernières auront des adresses IP dites privées (RFC 1918), généralement du type 192.168.*.*. Si vous êtes déjà

À L'ÉCOUTE DU RÉSEAU

En téléchargeant Wireshark et en l'installant comme une sonde filtrante sur un second PC à côté de votre poste de travail, vous pourrez découvrir le vrai contenu de vos échanges avec internet.

1

2

Release by TEAM-DZ

L'ASTUCE : CRÉEZ VOS PROPRES FILTRES

Pour construire un filtre automatiquement, il suffit de sélectionner un élément intéressant, comme une expression type ou une destination (URL), puis de choisir, dans le menu droit l'item *Apply as Filter/Selected*. Si vous ne connaissez pas la syntaxe, vous pouvez vous reporter au manuel en ligne (www.wireshark.org/docs). D'autres fonctions d'analyse aident à mettre en évidence les connexions d'un logiciel malveillant.

dans ce cas, il est possible que votre routeur soit en même temps un commutateur (ou switch) offrant plusieurs prises ethernet RJ45. Et si votre box offre une seule prise, vous y avez peut-être branché un commutateur, qui permet la connexion à internet de plusieurs machines simultanément. L'ennui est qu'un réseau commuté ne répète pas les paquets sur tous les brins. La sonde ne pourrait pas voir le trafic entre les autres machines et internet. La solution est de remplacer le commutateur par un concentrateur (ou hub). Si c'est le cas, passez l'étape suivante. Si vous ne disposez pas de hub, il faut configurer la sonde en pont (bridge).

3 Créez un pont (étape optionnelle)

Pour créer un pont, il faut deux cartes ethernet dans la sonde. Les deux interfaces doivent ensuite être configurée en pont, avec pour conséquence que le trafic arrivant sur l'une est répété sur l'autre. Dans le gestionnaire de connexions de Windows, sélectionnez les deux interfaces, puis choisissez dans le menu, en cliquant du bouton droit, l'option *Créer un Pont*. Une des interfaces sera connectée à la machine à surveiller, l'autre à la passerelle. Vérifiez que la machine suspecte se connecte bien au réseau à travers la sonde. Puis, sur cette dernière, lancez Wireshark.

4 Capturez des paquets critiques

Depuis la sonde, dans l'écran d'accueil de Wireshark, commandez le début de la capture de paquets en cliquant sur l'interface directement reliée à l'autre machine. Les paquets capturés sont affichés en temps réel avec, dans le panneau supérieur, leurs principales caractéristiques : heure, IP d'origine et de destination, protocole. Depuis le panneau inférieur, vous pouvez examiner les couches de protocole du paquet sélectionné. Vous accédez aux détails de chacune en dépliant les menus signalés par une flèche et situés à gauche de chaque item. Les informations les plus pertinentes pour la recherche d'activité de logiciels malveillants sont généralement situées dans la couche Internet Protocol et la couche d'application (HTTP, SMTP, DNS …). Mais que chercher dans cette avalanche de données ?

5 Sachez filtrer l'information

Tout d'abord, pour réduire le nombre de paquets à examiner, vous pouvez fermer quelques processus utilisant le réseau sur la machine testée. Il n'est peut-être pas utile d'avoir Bittorrent et le client de messagerie en tâche de fond, plus le navigateur collé sur une page bourrée de publicité. Pour identifier visuellement l'activité du réseau, Wireshark colore les lignes (correspondant à un paquet) suivant le protocole employé ou si les paquets ont un statut particulier (retransmission, fragment). Du point de vue de la recherche d'un logiciel malveillant, il faut faire attention aux adresses IP avec lesquelles la machine testée communique. Si on voit des requêtes DNS (bleu clair par défaut) vers une adresse IP différente des serveurs du fournisseur d'accès (visibles dans la connexion réseau), un fournisseur comme DynDNS ou No-IP, c'est suspect. Dans les autres cas, pour confondre une adresse IP anormale, il faut la résoudre en un nom de machine. Sélectionnez le paquet, puis dépliez complètement le menu *Internet Protocol* correspondant. Sur la ligne *Source* ou *Destination*, choisissez dans le menu l'option *Resolve Name*. S'il apparaît un nom de machine appartenant à un particulier (terminant par un nom d'opérateur grand public : proxad, orange, verizon …), ou située en Chine (nom finissant en .cn) ou en Russie (.ru) alors que vous ne visitez pas ces destinations, vous avez un élément de plus en faveur d'une infection.

6 Allez plus loin avec le filtrage avancé

Wireshark possède des possibilités de filtrage avancé. Dans le champ de recherche, situé juste sous la barre d'outils, vous pouvez entrer des expressions pour faire apparaître les paquets intéressants. Par exemple, *dns* ne laisse voir que les requêtes et les réponses DNS. **Philippe Roure**

3

4

5

6

Release by TEAM-DZ

Migrez vos données de communication

MOZBACKUP

60 minutes

Difficulté

Changer d'ordinateur induit forcément une migration des données, dont celles liées au client de messagerie et au navigateur web. Il existe pour cela des outils très astucieux et gratuit, comme MozBackup.

IL VOUS FAUT AUSSI...
- ✔ Une connexion internet
- ✔ Mozilla Thunderbird 3.1
- ✔ MozBackup 1.4.10

Vous êtes devenu un utilisateur inconditionnel du navigateur Firefox et du client de messagerie Thunderbird, et vous les utilisez sur plusieurs ordinateurs ? Alors vous allez adorer MozBackup, car il vous fera gagner un temps plus que précieux. En effet, lorsque vous utilisez un même logiciel sur plusieurs PC, vous perdez pas mal de temps à paramétrer l'application en fonction de vos besoins : c'est que l'on appelle le profil utilisateur. Mais plutôt que de répéter la manipulation sur autant de PC contenant Firefox ou Thunderbird, téléchargez MozBackup (http://mozbackup.jasnapaka.com/download.php) et installez-le. Il va se charger de récupérer automatiquement le profil utilisateur et les données liées à l'application. Le tout est ensuite astucieusement centralisé dans un seul et unique fichier que seul MozBackup sait interpréter. Selon le type de programme, le champ des possibilités n'est pas le même. L'outil se limite par exemple à récupérer les favoris, l'historique et les paramètres pour un navigateur internet. Avec un client de messagerie, ce sont les courriels, les pièces jointes et les paramètres qui seront ciblés. Tout cela se fait selon vos besoins. Il vous suffit simplement de cocher chacune des options proposées lors de la procédure de sauvegarde.

L'archive obtenue peut être restaurée sur n'importe quel ordinateur via la fonction d'importation de l'application. Il faut bien entendu avoir installé au préalable MozBackup et le programme ciblé par la sauvegarde. En plus d'être efficace et gratuit, MozBackup supporte de nombreuses applications open source. On trouve parmi elles Thunderbird, l'agenda libre Sundbird, le navigateur web Firefox et le gestionnaire de bibliothèque musicale Songbird. L'éditeur n'est compatible avec aucune application payante. Il ne vit que grâce à sa communauté d'utilisateurs et au bon vouloir de son éditeur. MozBackup s'appuie sur une interface ultra-intuitive qui se limite à un simple pas à pas. C'est à la portée de tout-un-chacun. Aucune connaissance informatique n'est ici nécessaire. ■

MODE D'EMPLOI EN 6 ÉTAPES

Un assistant intuitif et rapide MozBackup est une application open source compatible avec de nombreux navigateurs et clients de messagerie. Ce programme est proposé en libre téléchargement par son éditeur sur le site http://mozbackup.jasna paka.com/. Cet outil en anglais s'installe très rapidement sur l'ordinateur.

Choisissez l'application Faite votre choix entre restauration et sauvegarde puis définissez l'application cible. La première option va tout simplement récupérer l'ensemble des éléments (données, paramètres, etc.) et les regrouper automatiquement dans un fichier unique. Cliquez ensuite sur *Next*.

Release by TEAM-DZ

Définissez le profil à sauvegarder Lors de l'installation de Thunderbird, vous avez créé un profil utilisateur. Celui-ci regroupe l'ensemble de vos informations (paramètre du serveur, configuration de l'application, etc.). Cliquez sur votre profil, choisissez la destination du fichier de sauvegarde puis appuyez sur *Next*.

Informations à conserver Cette étape consiste à choisir les éléments à sauvegarder. Dans le cas d'un client de messagerie, MozBackup peut regrouper dans un seul et unique fichier les paramètres, les courriels, les mots de passe et les certificats liés à vos comptes. Cochez les cases selon vos besoins et cliquez sur *Next*.

Processus de sauvegarde Il faut compter une bonne vingtaine de minutes pour réaliser la sauvegarde de plusieurs milliers de courriels et des fichiers joints. Le fichier résultant a dans notre cas atteint les deux gigaoctets. Une archive bien utile qu'il est conseillé de mettre à l'abri sur une clé USB ou un disque dur externe.

Restaurez les données sur une seconde machine Il faut au préalable avoir installé MozBackup et la même version de Thunderbird. Surtout ne lancez pas celui-ci avant d'avoir réalisé la restauration des données. Exécutez MozBackup et choisissez l'option *Restore a profile*. La procédure est ensuite similaire aux précédentes étapes.

FRANCISEZ VOTRE APPLICATION

L'application disponible en téléchargement est uniquement proposée en anglais. Une lacune qu'il est facile de corriger avec un correctif proposé par l'éditeur sur son site. Celui-ci s'est appuyé sur la communauté d'utilisateurs pour traduire son application. On trouve donc au final un nombre important de traductions sous la forme d'un fichier à installer sur votre poste. Rendez-vous sur le site de l'éditeur dans la rubrique *Translations*. Sélectionnez le drapeau français pour lancer le téléchargement du fichier zip. Son poids étant très faible, l'opération ne prend que quelques secondes. Il vous faut décompresser l'archive avant toute autre manipulation. Ouvrez le dossier résultant et faites un glisser/déposer du contenu dans le répertoire de l'application. Cela va avoir pour effet de remplacer le fichier antérieur. Vous devez accepter le remplacement du fichier. Une fois la procédure finalisée, redémarrez le programme pour avoir accès à l'interface francisée.

Release by TEAM-DZ

Prenez le contrôle d'un PC à distance

TeamViewer

5 minutes

Difficulté

Les logiciels de prise de contrôle à distance vous donnent accès à toutes les fonctions d'un ordinateur distant, qu'il soit à l'autre bout de la pièce ou situé sur un autre continent. Démonstration.

La prise de contrôle à distance a toujours été la meilleure solution à la disposition des utilisateurs avancés pour dépanner, ou tout simplement accéder aux fichiers et aux applications d'un ordinateur distant. Que vous soyez un technicien ou un simple utilisateur, vous pouvez accéder aux données enregistrées sur le disque du PC sous contrôle ou lancer des applications comme si vous étiez devant l'écran. Le marché ne manque pas de solutions pour accomplir cette tâche, dont TeamViewer pour Windows. Le mode de fonctionnement de TeamViewer vous facilite vraiment l'installation, la configuration et la prise de contrôle. Ce logiciel fonctionne en mode client-serveur et les communications sont établies via le port 80 en http sécurisé ou pas selon le choix. Cette architecture, qui exploite le port dédié à l'internet, vous apporte une solution flexible et transparente pour l'administrateur réseau. En effet, elle permet de passer à travers les pare-feu et les serveurs Proxy en toute sécurité et sans perturber le fonctionnement du réseau.

TeamViewer propose plusieurs applications, mais son fonctionnement est le même : la connexion s'effectue vis un serveur qui centralise les demandes de connexions et met en relation l'hôte et son ou ses ordinateurs distants. Dans la version 6, le module client QuickSupport, conçu pour un accès rapide et direct des techniciens aux ordinateurs des utilisateurs, est optimisé grâce à des fonctions personnalisées qui s'adaptent aux besoins de l'entreprise. Il permet en outre de mettre en place des procédures de connexion automatique avec des clients référencés. Il est dévolu à la prise de contrôle, contrairement au module QuickJoin, qui permet d'organiser des réunions à distance avec prise de contrôle ou pas. Ce dernier se télécharge de façon indépendante et permet à plusieurs utilisateurs d'entrer simultanément l'identifiant du présentateur et de se connecter. C'est la solution idéale pour les présentations en groupe à distance, permettant à de multiples utilisateurs de se connecter et de rejoindre la réunion en même temps. Sans être aussi complets, d'autres logiciels gratuits, comme LogMeIn ou CrossLoop, offrent la possibilité de prendre la main sur un PC à distance. ■

MODE D'EMPLOI EN 6 ÉTAPES

Installez TeamViewer Pour prendre le contrôle d'un PC distant avec TeamViewer, vous devez téléchargez et installer le logiciel sur les deux postes. Cliquez sur la version que vous souhaitez installer, puis suivez les instructions qui s'affichent à l'écran. N'oubliez pas de cocher la case *Paramètres avancés* pour accéder à des réglages plus fins.

Définissez le type d'installation Cliquez sur *No* pour installer le logiciel pour des connexions entrantes et sortantes ponctuelles. Vous devrez à chaque utilisation lancer le logiciel et communiquer les coordonnées d'accès à votre correspondant. Si vous cliquez sur *Oui*, vous configurez le PC pour être accessible en permanence.

Release by TEAM-DZ

Paramétrez les accès à distance Ici vous réglez le contrôle en fonction de la confiance que vous avez dans l'opérateur distant, vous établissez des droits de modification complets ou soumis à votre approbation. L'autre choix proposé vous donne la main sur tout ce qui se passe sur votre PC.

Activez le VPN L'une des améliorations les plus notables de TeamViewer au cours de son évolution est l'adoption des liaisons sécurisées via le VPN. Cette fonction peut être utilisée sur deux postes distants, ou sur plusieurs postes dans le cas d'une conférence afin d'assurer la confidentialité des échanges.

Connexion au service La fenêtre de démarrage affiche les informations de connexion composées d'un identifiant (ID) et d'un mot de passe. Notez-les et communiquez- les à l'administrateur ou à la personne qui doit prendre le contrôle de votre PC. Il suffit d'inscrire ces informations dans la fenêtre de connexion et le logiciel fait le reste.

Prise de contrôle Lorsque vous établissez la connexion avec l'ordinateur distant vous avez le choix entre trois modes de connexion : contrôle à distance, échange de fichiers ou VPN. Vous pouvez changer de type de connexion en cours de route : passer du VPN à la prise de contrôle par exemple.

LES DÉCLINAISONS DE TEAMVIEWER

TeamViewer peut être téléchargé gratuitement pour la version basique ou moyennant le paiement d'une licence pour les versions payantes. Ces dernières fournissent, bien entendu, des fonctions plus évoluées ainsi que la possibilité de configurer des accès automatiques. Vous pouvez même personnaliser le module QuickSupport afin de le mettre aux couleurs de votre entreprise. Cette option est destinée aux professionnels de la maintenance à distance et de l'outsourcing informatique. Lors de la création des comptes QuickSupport personnalisés, indiquez-y les données de votre liste de partenaires distants. Dès que votre client démarre QuickSupport, il apparaît dans votre liste de partenaires et vous pourrez vous connecter d'un simple clic, sans avoir à échanger ni ID ni mot de passe par e-mail ou par téléphone. Vous pouvez également ajouter une clause de non-responsabilité personnalisée dans QuickSupport afin de vous protéger sur un plan juridique.
Vous pouvez maintenant définir vous-même le niveau de sécurité du mot de passe. Vous avez également la possibilité d'échanger des messages instantanés via QuickSupport et ce avant même d'établir la connexion TeamViewer et même si votre client n'a pas de compte ou de liste de partenaires.

Release by TEAM-DZ

Sauvegardez vos données en réseau

SyncBackSE

10 minutes

Initié

Ce logiciel de sauvegarde vous propose des fonctions complètes pour mettre vos données à l'abri. Il fonctionne en local ou en réseau et reconnaît même les serveurs FTP. Voici les étapes de sa mise en œuvre.

MODE D'EMPLOI EN 8 ÉTAPES

1

Téléchargez et installez SyncBack Ce logiciel de sauvegarde existe dans plusieurs versions dédiées à des usages différents, ici nous avons installé la version basique, SyncBackSE 5.9.4.0. Après installation, vous devez d'abord créer un profil de sauvegarde. Cliquez sur le menu *Profils* pour lancer la procédure.

2

Créez un profil de sauvegarde SyncBackSE peut gérer plusieurs tâches de sauvegarde. La fenêtre de paramétrage s'ouvre pour vous permettre de nommer votre profil. Choisissez un nom qui décrit la tâche avec le plus de précision possible afin de savoir exactement ce que contient la sauvegarde.

3

Choisissez le type de sauvegarde SyncBackSE propose plusieurs types de sauvegarde qui s'adaptent à tous les besoins. Pour une sauvegarde simple, choisissez *Sauvegarde*, sinon cliquez sur l'option qui vous intéresse. Sachez que chaque option agit différemment selon la configuration établie.

4

Sauvegarde sur FTP En plus des supports locaux et ceux situés sur le réseau, SyncBackSE vous propose la sauvegarde sur les serveurs FTP. Si vous choisissez cette option, préparez les informations relatives au serveur (nom, identifiant et mot de passe), sinon cliquez sur *Pas de FTP* puis *Suivant*.

Release by TEAM-DZ

Identifiants du FTP Lorsque vous choisissez une sauvegarde sur FTP, cette fenêtre s'affiche pour vous permettre d'entrer toutes les informations relatives au serveur distant. Allez dans *Configuration manuelle* et entrez les informations relatives à votre serveur, puis testez-les pour plus de sûreté.

Déterminez la fragmentation Les options proposées dans cette fenêtre règlent le mode de stockage des fichiers de sauvegarde et leur compression ou pas. Cette option vous permet de fragmenter la sauvegarde en fichiers plus petits afin de respecter les limitations de taille sur certains supports.

Indiquez la source et la destination Durant cette étape, vous allez indiquer au programme les fichiers source ainsi que le support et le répertoire de destination des sauvegardes, que ce soit en local ou sur le réseau. Cliquez sur les icônes à gauche et choisissez l'emplacement de la sauvegarde.

Simulez votre sauvegarde Une fois que vous avez fini de créer la sauvegarde, SyncBackSE affiche cette fenêtre qui résume la configuration de votre sauvegarde ainsi que les options choisies. Cliquez sur *Simulation* pour valider vos choix ainsi que les fichiers et répertoires source et destination.

QUEL TYPE DE SAUVEGARDE ADOPTER ?

SyncBack est un petit logiciel gratuit, téléchargeable sur www.syncback.fr, mais assez complet quant à ses fonctions de sauvegarde et sa compatibilité. Il vous propose plusieurs types de sauvegardes qui se distinguent les unes des autres et dont il faut connaître les caractéristiques pour bien utiliser le logiciel. La sauvegarde simple, par exemple, vous permet de seulement copier vos fichiers dans un endroit sécurisé, elle peut être automatique ou manuelle. La synchronisation agit différemment en effectuant la copie des fichiers dans les deux directions afin de maintenir deux copies identiques. La sauvegarde en miroir copie les fichiers de la source vers la destination afin de maintenir une copie exacte de la source, mais cette fonction efface les fichiers et répertoires du support de destination s'ils ont été supprimés de la source. Enfin, la dernière option, *Group*, vous permet de regrouper plusieurs profils afin qu'ils se lancent en même temps, ce qui vous évite de les activer un par un.

Release by TEAM-DZ

MATÉRIEL REQUIS
Photos

NIVEAU
Facile

QUESTION

La dernière version de Picasa reconnaît automatiquement les visages. Comment l'aider à regrouper les photos dans des dossiers au nom des différentes personnes ?

Regroupez les photos de vos proches

> Des albums au nom des personnes reconnues Téléchargez Picasa à partir de la page http://picasa.google.fr. Une fois le logiciel installé, indiquez-lui les dossiers dans lesquels se trouvent vos photos : passez par la commande *Fichier > Ajouter un dossier à Picasa*. Pour identifier quelqu'un, diquez dans la zone *Ajouter un nom sous la vignette d'un visage* et entrez le nom de la personne. La fenêtre d'identification s'ouvre. Cliquez sur *Nouveau contact*. Modifiez éventuellement son nom et son pseudo. Cliquez sur *OK*. Un nouvel album au nom que vous avez entré est créé dans la collection *Personnes*. C'est là que Picasa, au fur et à mesure de son investigation dans vos albums, introduira la vignette de toutes les photos représentant la même personne. Pour ignorer quelqu'un, diquez sur le bouton *X* de sa vignette. Il arrive que Picasa se trompe en introduisant dans un album la photo de quelqu'un d'autre. Cliquez du bouton droit sur la vignette à corriger. Si la personne n'a pas encore été identifiée, choisissez la commande *Déplacer vers une nouvelle personne*. Si la personne a déjà été identifiée (elle a donc un album à son nom), choisissez plutôt la commande *Ajouter à l'album dédié à la personne* puis sur un nom.

À LIRE

Google est à vous
Plus de 300 pages sur la recherche, les applications et les services en ligne de Google : Google Earth, Google Maps, Picasa, Google Docs, Google Chrome, Google Reader, Blogger, FeedBurner, Google Desktop, les API cartographiques, Google Mobile, Google Agenda... Beaucoup d'explications pratiques, d'astuces et de conseils pour utiliser toutes les ressources de chacun des services et des programmes.
Auteur Jean-Noël Anderruthy
Éditeur Eni
Prix 20,95 €

MATÉRIEL REQUIS
Windows

NIVEAU
Facile

QUESTION

Dans la fenêtre d'invite de commande, ouvrez le menu *Système* (en cliquant dans le coin supérieur gauche de la fenêtre) et choisissez la commande *Propriétés*. Seules deux polices sont disponibles : Lucida et Polices raster. Comment ajouter d'autres polices ?

Multipliez les polices dans l'invite de commande

> La Base de registre Lancez regedit, l'éditeur de la Base de registre. Sélectionnez la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Console\TrueTypeFont*. Elle contient une seule valeur chaîne nommée 0 et contenant comme donnée le nom de police Lucida Console. Ajoutez une valeur chaîne : la commande est dans le menu *Édition*. Nommez-la *00* et entrez comme donnée le nom d'une police de caractères installée sur votre PC. Si vous ajoutez encore d'autres polices, donnez-leur comme nom *000*, *0000*, *00000*. Pour connaître le nom des polices installées sur votre PC, ouvrez le module *Polices* du Panneau de configuration. Pour voir à quoi ressemble une police, double-cliquez sur son icône. Il existe deux grandes familles de polices : monospaces et proportionnelles. Dans une police monospace, chaque caractère occupe le même espace en largeur. En revanche, lorsque la police est proportionnelle, les caractères occupent l'espace qui correspond à leur largeur. Par exemple, dans une police monospace, le « i » et le « m » occupent la même largeur.

Release by TEAM-DZ

Windows news répond à vos questions et analyse les problèmes que vous rencontrez dans l'usage quotidien du nouveau Windows.

WINDOWS 7 ET SES BUGS

UNE IMPRESSION DÉVOREUSE DE CPU

Q ***J'ai upgradé mon ancien PC de Windows Vista à Windows 7. Depuis, mes impressions prennent un temps considérable, et la machine rame de façon impressionnante. Une réinitialisation du spool d'impression n'a eu aucun effet. Le problème est récurrent mais pas systématique.***

R Vous êtes probablement face à un bug récemment découvert par Microsoft, qui affecte l'impression sous Windows 7 sur des machines monocœur. Ce bug n'est pas systématique, mais se traduit par une utilisation à 100 % du processeur, d'où le ralentissement constaté. Le bug se situe au niveau du spooleur d'impression. Un correctif a été mis au point, mais celui-ci n'est communiqué qu'à la demande par le support Microsoft. Pour plus d'informations, recherchez l'article *2295825* dans la *Knowledge Base* Microsoft. Sachez aussi que ce bug sera corrigé par le SP1 de Windows 7. ■

WINDOWS 7 ET SON MBR

RÉPAREZ LE BOOT

Q ***J'ai voulu installer un multiboot sur mon PC. Résultat des courses, plus rien ne marche et mon PC sous Windows 7 tout neuf refuse de démarrer. J'obtiens un message d'erreur au boot. Comment puis-je récupérer mon accès à Windows?***

R Votre MBR (Master Boot Record) a probablement été endommagé. C'est souvent le cas lorsque l'on essaye d'installer un ancien Linux ou un ancien Windows en double boot. Pour résoudre le problème, il vous faut le DVD de Windows 7 ou au moins le CD de réparation système. Rappelons que pour générer un tel CD de secours, il suffit de taper « réparation » dans le menu *Démarrer* et de suivre l'assistant de création du disque de réparation système. Dans votre cas, il est trop tard pour générer un tel CD. Si vous n'avez le DVD de Windows 7, vous pouvez l'obtenir pour quelques euros via le site officiel SystemDiscs.com.
Démarrer votre PC depuis le CD (ou DVD Win7). Choisissez *Réparer l'ordinateur* (selon la version du CD). Sélectionnez l'installation de Windows proposée (celle du disque C:), cliquez sur *Suivant* et choisissez *Réparation du Démarrage*.
Si vous n'aimez pas les processus automatiques, vous pouvez aussi sélectionner *Invite de commandes* et saisir la commande *bootrec /fixboot*. Si vous avez installé un Windows XP en double-boot et souhaitez retrouver le boot de Windows 7, utilisez la commande *bootsect/nt60 all*. ■

L'ASTUCE À RETENIR

WINDOWS 7 ET LE BRUIT

CPU AMD & VENTILATION

Q ***J'ai récupéré un Tablet PC HP. J'aime bien la machine, et ses performances sont très au-delà de mes besoins bureautiques. Le mode Tablet PC de Windows 7 est fabuleux, avec ses derniers écrans tactiles. Malheureusement, je trouve cette machine bruyante, le processeur AMD chauffant trop et obligeant la ventilation à fonctionner au maximum. Je n'ai rien trouvé dans le BIOS qui me permette de la contrôler. Auriez-vous une idée?***

R AMD propose sur son site un outil de pilotage de l'OverClocking (maximiser les performances) de ses processeurs. Cet outil peut également être utilisé pour « UnderClocker » (autrement dit minimiser les performances) le processeur. Dès lors, il se met à moins chauffer et la ventilation fonctionne au ralenti (donc plus silencieusement). Comme tous les outils de ce genre, il faut faire très attention à ce que vous faites. Booster un processeur n'est jamais sans conséquence sur l'électronique.

Vous pouvez télécharger le programme OverDrive Utility depuis le site AMD (**http://bit.ly/ateKuq**). Il comporte plusieurs onglets, dont un dédié à la performance et l'autre dédié à la ventilation. Seul bémol, le logiciel n'est pas compatible avec tous les Chipsets AMD (les modèles antérieurs au 760G ne sont pas supportés) et ne fonctionne évidemment pas avec les chipsets non-AMD. ■

WINDOWS SERVEUR

FORMATAGE EXTERNE IMPOSSIBLE

Q ***Le problème ne concerne pas directement Windows 7 mais son cousin Windows Server 2008 R2. J'ai ajouté à ce serveur un disque dur externe en USB pour réaliser des sauvegardes faciles à transporter en un autre lieu. Mais dès que j'essaye de le formater, j'obtiens une erreur.***

R Vous êtes en train de forcer le formatage en NTFS d'un périphérique amovible, ce qui n'est pas toujours possible (tout dépend des stratégies définies). Pour réparer ce souci, aussi valable sous Windows 7, vous pouvez formater le disque dur sur une autre machine ou procéder ainsi: Ouvrez le menu *Démarrer*, cliquez du bouton droit sur *Ordinateur* et sélectionnez *Gérer*. Allez dans *Stockage > Gestion des disques*. Cliquez du bouton droit sur le disque incriminé dans la liste inférieure (cliquez bien sur le disque et non la partition) puis demandez les *Propriétés*. Allez dans l'onglet *Stratégies*. Cochez *Meilleures performances*. Validez avec *OK*. Maintenant, cliquez du bouton droit sur la partition et sélectionnez *Formater*. ■

Release by TEAM-DZ

WINDOWS 7 & SES PROTECTIONS

ACTIVATION IMPOSSIBLE

Q ***L'installation de Windows 7 s'est bien passée mais il m'est impossible d'activer la version. C'est un Windows 7 authentique. J'ai juste fait la bêtise de ne pas l'activer tout de suite mais quelques jours après, alors que j'avais déjà installé plein d'applications…***

R Tout dépend de la cause de dysfonctionnement. En supposant que la clé soit valide et authentique, le problème provient alors très probablement d'un accès restreint à la Base de registre, peut-être provoqué par votre antivirus. Ouvrez le menu *Démarrer*, saisissez *CMD* et validez avec [Ctrl]+[Shift]+[Entrée]. L'invite de commande s'ouvre en mode administrateur. Saisissez la commande *slmgr -ato* et validez avec [Entrée]. Si vous obtenez l'erreur *Données invalides – Code Erreur: 8007000d*, vous êtes dans la situation où la clé *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root* a vu ses permissions altérées. Le plus simple est de télécharger le programme correctif proposé par Microsoft sous la référence *Fix It 50485* (http://support.microsoft.com/kb/2230957/). ■

WINDOWS 7 & SES PERFORMANCES

UN POINT SUR READYBOOST

Q ***Je cherche à améliorer les performances de mon PC et je me demandais si ReadyBoost pouvait être une solution viable ?***

R ReadyBoost n'accélère pas vraiment « le PC » mais peut donner de sérieux coup de fouet à certaines applications. Ainsi, nous avons noté des gains de performances importants (de 20 à 60 %) sur des applications gourmandes, comme celles d'Adobe (Premiere, Audition, Flash), Windows Media Player, Windows Media Center ou Zune. Introduite avec Vista, et sans que personne ne dénote réellement son utilité, cette technologie a considérablement évolué sous Windows 7. ReadyBoost s'active simplement en insérant une clé USB dans son PC et en sélectionnant l'option *Accélérer mon système*. On peut aussi y accéder via les propriétés du lecteur et son onglet *ReadyBoost*. Pour que les effets de ReadyBoost soient réellement sensibles, il faut plusieurs conditions : tout d'abord, votre clé USB doit être extrêmement rapide. L'idéal est d'opter pour des clés estampillées du logo « Enhanced for ReadyBoost ». Ensuite, votre clé doit au moins posséder une capacité de 1 Go. En réalité, ReadyBoost n'est efficace que si l'espace ReadyBoost est au moins deux fois supérieur à votre mémoire RAM. Donc si vous avez 3 Go de RAM, il faudra une clé de 8 Go minimum. Notez que plus la clé est rapide, meilleurs sont les gains. Comme les clés les plus véloces sont souvent celles de moindre capacité, il est en pratique préférable d'utiliser deux clés de 4 Go dédiées à ReadyBoost. Car, désormais, sous Windows 7, ReadyBoost sait utiliser plusieurs clés simultanément. La taille mémoire maximale d'une clé ReadyBoost est de 32 Go. Et la technologie supporte jusqu'à huit clés simultanées, ce qui nous amène à une mémoire ReadyBoost maximale de 256 Go. Enfin, signalons que ReadyBoost se désactive automatiquement sur la plupart des PC dotés en standard de disques SSD. Pour être complet, sachez qu'il est désormais possible de contrôler l'activité de ReadyBoost. Ouvrez l'*Analyseur de performances*, diquez sur *Ajouter des compteurs*, et ajoutez *Cache ReadyBoost*. L'outil va vous permettre de surveiller l'activité de cette fonction dans ses moindres détails et déterminer sur quelles applications son impact est le plus important. ■

WINDOWS 7 & SA PERSONNALISATION

TOUJOURS PLUS DE THÈMES

Q ***J'ai constaté que vous utilisiez une grande variété de thèmes de bureau pour vos captures d'écran. D'où proviennent-ils et comment y accéder ?***

R Il n'y a aucune magie derrière cette variété. Tous ces superbes fonds d'écran sont fournis par Microsoft et accessibles à tous. Une partie d'entre eux provient de thèmes « nationaux » (Windows 7 propose des thèmes adaptés à chaque pays), d'autres sont des bonus. Quoi qu'il en soit, tous sont aujourd'hui accessibles depuis le site Microsoft dédié à Windows 7. Pour y accéder, rien de plus simple : diquez du bouton droit sur le bureau et sélectionnez *Personnaliser*. Dans la fenêtre de personnalisation des thèmes, notez la présence d'un lien *Obtenir plus de thèmes en ligne*. Cliquez dessus. Cette option vous amène directement sur l'espace dédié à Windows sur le site Microsoft. Notez que les thèmes proposés peuvent varier selon les pays. Si vous allez sur la version américaine (http://bit.ly/axe46A), vous découvrirez une sélection légèrement différente avec davantage de nouveautés (comme les nouveaux thèmes Lightning, Halloween, ou encore Best of Bing 4). Vous trouverez également plein d'autres contenus superbes pour personnaliser votre PC sur l'autre site officiel de Microsoft : www.personnalisez-votre-pc.com. ■

Release by TEAM-DZ

WINDOWS 7 ET SES BUGS

UN RENOMMER PÉTRIFIANT !

Q ***Depuis quelque temps, chaque fois que j'essaye de renommer un fichier depuis l'explorateur, Windows se fige durant un très long moment avant de rendre la main.***

R Ce phénomène se produit lorsque l'on a beaucoup de fichiers sur son disque. Au moment de renommer un fichier, Windows vérifie si celui-ci est ouvert. Cette vérification peut prendre parfois beaucoup de temps et tout l'ordinateur semble alors figé. Microsoft a publié un correctif à ce problème, qui trouve son origine dans Vista et qui a survécu jusque dans Windows 7. Pour obtenir ce patch, allez sur la page KB980382 (http://support.microsoft.com/kb/980382/) du support et demandez l'accès au correctif en remplissant le formulaire. ■

RÉPAREZ WINDOWS 7

RÉINSTALLER POUR RÉPARER?

Q ***Mon Windows 7 fait preuve de comportements erratiques probablement dus à des pilotes que j'ai installés sans grande rigueur. Peut-on réinstaller Windows 7 dans un mode « réparation » comme cela existait sous Windows XP?***

R La réponse courte à votre question est « pas vraiment ». Mais on peut la nuancer. Il est possible de réparer une installation qui ne démarre plus en redémarrant le PC depuis le DVD de Windows 7 et en sélectionnant *Réparer l'ordinateur* sur le premier écran. Il est aussi possible de réparer un Windows 7 erratique en le réinstallant à condition de pouvoir lancer ce Windows 7 et l'utiliser un minimum. Dans ce cas, insérez le DVD de Windows 7 dans le lecteur et procédez à une Mise à jour (car vous demandez bien une mise à jour de Windows 7 vers Windows 7). Cette opération réinstalle Windows 7 en conservant paramètres et applications comme le faisait l'ancienne Réparation de Windows XP. En revanche, si Windows 7 n'est pas suffisamment opérationnel pour lancer le DVD, vous devrez refaire une installation à neuf en démarrant l'ordinateur depuis le DVD de Windows 7. Si vous ne demandez pas de reformatage du disque, cette installation ne détruira aucun fichier et document personnel. Mais vous devrez réinstaller les programmes et reprogrammer vos paramètres personnels. ■

L'ASTUCE À RETENIR

RACCOURCIS CLAVIER

MAÎTRISEZ LES EXTINCTIONS

Q ***Y a-t-il un raccourci clavier pour éteindre Windows 7, le mettre en veille, changer d'utilisateur, bref un raccourci clavier pour les options du menu Arrêter ?***

R Non, il n'existe pas de raccourcis de fermeture sous Windows 7. Le raccourci [Windows] + [L] permet de changer d'utilisateurs. [Alt] + [F4] permet de fermer une à une toutes les applications jusqu'à finalement fermer Windows et son Bureau. Mais cela ne répond pas à vos besoins. Deux choses peuvent toutefois résoudre votre problème. La première consiste à attribuer des comportements différents aux boutons *Power*, *Veille* et *fermeture d'écran* de votre ordinateur portable. Saisissez *boutons* dans le menu *Démarrer* et sélectionnez *Modifier le comportement des boutons d'alimentation*. Vous pouvez alors sélectionner des fonctions différentes (veille, veille prolongée, etc.) pour chaque bouton. L'autre solution consiste à télécharger et installer un petit outil gratuit dénommé *ShutDownAfter*. Il permet d'attribuer des raccourcis clavier différents aux fonctions *Arrêter*, *Mettre en veille*, *Veille prolongée*, *Redémarrer* et *Fermer la session*. *ShutDown After* de VCS est librement téléchargeable depuis l'URL : *www.vcsoftwares.com/sa.html*. ■

WINDOWS 7 & INTERNET

SAUVEGARDEZ IE9

Q ***Je cherche un moyen simple de sauvegarder toutes mes données Internet Explorer (comme l'auto-complétion, les cookies, mes paramètres de sécurité personnalisés). Je voudrais en effet à la fois les transférer sur mon portable et réinstaller mon PC de bureau.***

R Deux solutions possibles : utiliser un disque externe ou l'application *Transfert de fichiers et paramètres Windows* (saisissez *Transfert* dans le menu *Démarrer*). Vous pourrez alors choisir de ne réimporter que les paramètres d'IE. Il existe, toutefois, une solution bien plus pratique et efficace : BackRex. Compatible IE 6, 7, 8 et même IE9, cette application gratuite sauvegarde à la demande ou de façon régulière vos Favoris, vos paramètres Proxy, vos zones de sécurité, vos personnalisations, vos cookies, votre historique, et l'autoremplissage des formulaires. L'utilitaire BackRex est librement téléchargeable depuis l'URL : www.backsettings.com/internet-explorer-backup.html. ■

Release by TEAM-DZ

WINDOWS 7 ET GROUPE RÉSIDENTIEL

MOT DE PASSE PERDU ?

Q ***Je viens de recevoir un PC portable sous Windows 7. J'ai déjà passé mes autres PC du foyer en Windows 7. Ce portable me demande le mot de passe du Homegroup (groupe résidentiel). Je ne m'en souviens plus. Comment le retrouver ?***

R Le groupe résidentiel est destiné à simplifier la mise en réseau de machines. La première fois que l'on installe un PC en Windows 7, le système propose de créer un *Groupe résidentiel* et, pour cela, de saisir un mot de passe. Cette machine deviendra la machine « maître » de ce groupe. Lorsqu'on installe d'autres PC en Windows 7 sur le réseau, le système reconnaît l'existence d'un groupe résidentiel et vous propose de le rejoindre en saisissant le mot de passe défini lors de la création du groupe sur la machine maître. Si vous avez oublié ce mot de passe, allez sur une des machines reliées au groupe, ouvrez le menu *Démarrer*, saisissez *Groupe* et sélectionnez *Groupe Résidentiel*. Cliquez alors sur *Afficher ou imprimer le mot de passe du groupe résidentiel*.

WINDOWS 7 ET MISE À JOUR

LES DÉBOIRES DE WINDOWS UPDATE

Q ***J'avais déjà pas mal de souci avec Windows Update sous XP. À mon grand désespoir, j'en rencontre autant aujourd'hui sous Windows 7 (je suis en 64 bits) avec des mises à jour qui plantent à leur installation et se redéclenchent à chaque démarrage. À quoi sont dus ces problèmes et quel espoir puis-je avoir de m'en sortir ?***

R Depuis toujours, nombreux sont les utilisateurs qui rencontrent des soucis avec Windows Update. La plupart du temps, cela se produit suite à des infections par des spywares ou après l'usage d'outils de nettoyage ou d'optimisation qui éteignent parfois des services ou touchent à des clés de registre essentielles à Windows Update. Plusieurs choses peuvent être essayées lorsque Windows Update devient récalcitrant. Si vous recevez une erreur « 0x80070643 » (ou 643), téléchargez le réparateur FixIt (http://go.microsoft.com/?linkid=9740433). Si vous recevez une erreur «0 x 80070002» ou «0 x 80070003», utilisez l'outil de réinitialisation du Windows Update (http://go.microsoft.com/?linkid=9665683). Si l'erreur n'est pas signalée, essayez de télécharger et de lancer l'outil de réparation de Windows Update dénommé System Update Readiness Tool de Microsoft (selon les cas, soit en version 32 bits - http://bit.ly/9xJjpM - soit en version 64 bits - http://bit.ly/bCvLqe). Normalement, cet outil répare les clés et les droits d'accès détériorés qui gênent le bon fonctionnement des mises à jour.

Il existe une dernière solution, si seule une mise à jour refuse à l'infini de s'installer. C'est souvent le cas de pilotes inadaptés à votre PC pour un périphérique mal détecté. Elle consiste à tout simplement demander à Windows Update de ne plus tenir compte de cette mise à jour automatique. Ouvrez le menu *Démarrer*, saisissez *Update* dans le champ de recherche puis cliquez sur *Windows Update*. Si tout est à jour, le panneau de configuration doit indiquer qu'une mise à jour reste disponible. Dirigez-vous sur le lien pour afficher l'écran de sélection des mises à jour « importantes » ou « facultatives » disponibles. Cliquez du bouton droit sur la mise à jour perturbatrice et sélectionnez *Masquer la mise à jour*. Faites *OK*. Cliquez sur *Recherchez les mises à jour* et réalisez les éventuelles mises à jour demandées puis redémarrez le PC. ■

WINDOWS 7 ET SES TÂCHES

TUEZ PLUSIEURS APPLIS

Q ***J'ai installé un adware/spyware par inadvertance. Mais je n'arrive pas à le retirer, pas plus que mon antivirus AVG. Le problème, c'est que le spyware utilise trois processus simultanés qui se vérifient mutuellement et se relancent entre eux dès que j'en éteins un. Comment tuer tous les programmes en mémoire d'un seul coup ?***

R Sous Windows 7, il existe la commande *TASKKILL* pour tuer une ou plusieurs tâches actives simultanément, ce qui permet ensuite d'aller effacer les exécutables (notamment en cas d'infection). Il faut cependant spécifier le nom d'utilisateur dans la commande. Il est toujours possible de le connaître via le menu *Démarrer*, ou en regardant la colonne *Nom d'utilisateur* dans l'onglet *Processus* du Gestionnaire des tâches ([CTRL] + [Shift] + [ESC]). Supposons que l'utilisateur se nomme WinNews. Pour tuer toutes les tâches, il suffit de lancer la commande *TASKKILL/F/FI "USERNAME eq WinNews"* (en la saisissant depuis l'invite de commandes ou directement depuis le champ de recherche du menu *Démarrer*). Cela dit, cette commande va également « tuer » le bureau et Aero. Pour éviter ce problème, il faut compléter la commande en y introduisant des exclusions. La commande devient alors : TASKKILL/F/FI" USERNAME eq WinNews"/FI "IMAGENAME ne explorer.exe" /FI "IMAGENAME ne dwm.exe". ■

Release by TEAM-DZ

WINDOWS 7 & L'UAC

L'UAC EN RESTE FIGÉ !

Q ***J'essaie de changer les paramètres UAC, mais une fois la modification réalisée la fenêtre refuse de se fermer et le réglage n'est jamais validé !***

R Il s'agit d'un bug connu provoqué par… Office 97 ! Nous ne pouvons donc formuler ici que deux conseils imparables : vous devriez vraiment passer à Office 2010 ; Office 97 a largement fait son temps et vous avez amplement rentabilisé votre investissement de l'époque…Il est temps de retourner dans l'univers de la bureautique du XXIe siècle ! Des produits aussi anciens n'ont jamais été prévus ni testés sous Windows 7.En attendant d'acquérir Office 2010, Microsoft a eu la bonne idée de produire un patch « FixIt » qui corrige le problème. À télécharger ici : http://go.microsoft.com/?linkid=9714720 ■

WINDOWS 7 & SES GADGETS

GADGETS RÉCALCITRANTS

Q ***Mes gadgets Windows 7 ne fonctionnent plus. Impossible de les poser sur le Bureau. Ils restent comme figés à mi-distance, apparaissant plus comme des fantômes et ne fonctionnant pas. J'ai essayé de désinstaller tous les gadgets, mais rien n'a changé.***

R Plusieurs choses peuvent être responsables d'un dysfonctionnement des gadgets sous Windows 7. La première raison, et la plus simple à corriger, est souvent l'activation de l'UAC. Les gadgets nécessitent que l'UAC soit activée. Dans le menu *Démarrer*, saisissez *contrôle compte* et remontez l'ascenseur d'un cran. La deuxième cause la plus fréquente est un dysfonctionnement au niveau même du gestionnaire de gadgets. Il faut alors le réinitialiser. Pour cela, commencez par lancer *Registry* depuis le champ de recherche du menu *Démarrer*. Déployez la clé *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Sidebar* et supprimez-la avec tout son contenu (en cliquant du bouton droit sur *Sidebar*). Fermez l'éditeur de la Base de registre. Ouvrez le *Gestionnaire des tâches* puis l'onglet *Processus*, cochez *Afficher les processus de tous les utilisateurs*, cliquez sur *Sidebar.exe* puis sur *Arrêter le processus*. Ouvrez *l'invite de commandes* en mode administrateur et exécutez la commande *DEL "%localappdata%\Microsoft\Windows Sidebar"/s*. Redémarrez le PC et réinstallez vos gadgets ! ■

L'ASTUCE À RETENIR

WINDOWS 7 & SES THÈMES

CHANGEZ DE LOOK

Q ***Je cherche une astuce pour faire varier le look des fenêtres de Windows 7 en fonction des heures de la journée, un peu comme je le fais avec le papier peint du bureau grâce à la fonction de changement d'images automatique intégrée. Savez-vous si une telle solution existe ?***

R Nous ne connaissons pas vraiment d'outils qui répondent directement à votre besoin. Mais vous pouvez tout de même trouver quelques utilitaires qui permettent simplement, et sans trop alourdir le système, de modifier à volonté l'apparence des fenêtres.
En l'occurrence, AeroWheather n'est vraiment pas très loin de réaliser ce que vous demandez. Mais au lieu de faire varier les couleurs des fenêtres en fonction de l'heure, il les modifie en fonction de la météo ! AeroWheather est gratuit et téléchargeable à l'adresse : **http://bit.ly/gqHDQS**.
Une autre solution, plus radicale et spectaculaire, consiste à installer le logiciel CustoPack Tools de CrystalXP. Fonctionnant en 32 et 64 bits, il permet de personnaliser et de complètement transfigurer l'aspect du bureau et des fenêtres… Le site propose toute une galerie de thèmes et d'habillages à télécharger. CustoPack Tools est un logiciel gratuit que vous pouvez télécharger à cette URL : **www.custopack.com/en/download**. ■

WINDOWS 7 & SES PÉRIPHÉRIQUES

RECONNAISSANCE EN PANNE

Q ***Mon Windows 7 semble ne plus reconnaître certains périphériques que je lui connecte et me signale que le périphérique ne fonctionne pas correctement. Il fonctionne pourtant très bien sur une autre machine Windows 7…***

R A priori, ça n'est pas directement lié aux drivers à moins que les périphériques en question ne disposent pas de pilotes 64 bits (si le PC qui tourne est en 32 bits et que celui qui ne fonctionne pas est en 64 bits, la cause est probablement celle-là). Les autres motifs de ces dysfonctionnements peuvent être nombreux et dépendent beaucoup des logiciels lancés sur votre ordinateur, notamment des outils d'optimisation système et des éventuels « pseudo-nettoyages » qu'ils ont pu réaliser en Base de registre. Microsoft a repéré différentes situations menant à ces problèmes et a produit un outil de réparation « FixIt ». Dénommé « *Automated Troubleshooting Services 1.0* », et surnommé « *Mats* », il est à télécharger sur http://go.microsoft.com/?linkid=9740816. ■

Release by TEAM-DZ

WINDOWS 7 AU DÉMARRAGE

AU CŒUR DES AUTORUNS

Q ***Une étrange application se charge au démarrage mais je n'arrive pas à voir quelle zone système l'exécute ainsi automatiquement. Avez-vous une idée, sachant que j'ai déjà fouillé dans le dossier* Démarrage *et dans les clés Run et RunOnce?***

R En réalité, les zones du système qui permettent d'autodémarrer des applications sont plus nombreuses que l'on ne le croit, et elles ne sont pas toutes faciles à dénicher et à parcourir. Heureusement, deux outils plutôt destinés aux utilisateurs avertis permettent de les explorer et de décocher les éléments dont on n'a pas besoin. Le premier s'avère très connu puisqu'il s'agit du célèbre Autoruns de SysInternals (live.sysinternals.com). Le second est plus récent et explore des zones du système encore plus singulières, à la recherche d'éléments autodémarrés. Il se nomme AutoStart Explorer de Mischel Internet Security, l'éditeur de TrojanHunter (www.misec.net/products/autostartexplorer). Avec ces deux outils, vous serez bien armé pour résoudre le problème. ■

WINDOWS 7 ET SES MANQUES

DES OUTILS D'ADMINISTRATION

Q ***Pouvez-vous m'expliquer pourquoi le gestionnaire de services ou l'observateur d'événements de Windows 7 sont toujours aussi austères et peu pratiques alors même que tout le reste du système, y compris le panneau de configuration possède des fonctions de recherche et de filtrage? En tant qu'administrateur informatique d'une TPE, je passe ma vie sur ces deux fonctions.***

R La création d'un système aussi évolué que Windows 7 est une question de compromis et de gestion des priorités. Les équipes de Microsoft travaillent sans cesse sur des améliorations qui ne peuvent pas toujours être intégrées dans le système dans les temps impartis. Microsoft prévoyait effectivement d'améliorer cette partie du système, mais la priorité a été donnée aux fonctions utilisées par le plus grand nombre. Heureusement, vous n'êtes pas sans solutions. Technet regorge souvent d'idées, de conseils et d'outils utiles pour des administrateurs tels que vous. Je vous invite à consulter ce site quotidiennement et à vous abonner à ses nombreux flux RSS. Toute une partie de Technet est en effet dédiée à des blogs tenus par des ingénieurs de Microsoft ou des partenaires proches de Microsoft (les MVPs). Et l'on peut souvent y dénicher des perles. À l'instar du blog de Sateesh Arveti ou de Systinternals (une autre source d'utilitaires de Microsoft), ce MVP propose de nombreux outils pratiques pour améliorer la vie de l'administrateur. Parmi cette collection, deux utilitaires devraient retenir votre attention* : *Services Explorer* (http://bit.ly/fHK7X9) remplace avantageusement l'outil « Services.msc » et offre une navigation avancée dans les services du système, avec des filtres basés sur divers critères tout en permettant de vérifier les dépendances liées à chaque service. Il permet aussi de démarrer ou d'arrêter les services, mais surtout de les désinstaller s'ils ne vous sont d'aucune utilité ! ■

* Dans un même ordre d'idées, « Enhanced Event Viewer » (http://bit.ly/gYILx3) fait office d'observateur d'événements dont vous avez toujours rêvé ! Il permet de naviguer beaucoup plus facilement et efficacement dans les journaux de *Windows*. On y trouve ainsi des filtres bien plus immédiats que ceux de l'observateur et surtout, il procure cette fonction de recherche qui fait si cruellement défaut à l'outil standard. Signalons également que Sateesh Arveti a aussi produit des utilitaires équivalents pour améliorer le gestionnaire des tâches Windows Media Player, ou surveiller le temps passé sur chaque application (Application Watcher).

WINDOWS SERVER 2008 R2

PAS DE DRIVERS POUR LA VIDÉO

Q ***Suite à votre dossier sur Windows Server 2008 R2, j'ai entrepris d'installer la version d'évaluation sur un PC récent et bien dimensionné. Mais le système ne veut pas reconnaître la carte ATI Radeon HD 4670 qui est dedans et se contente du driver VGA standard. J'ai téléchargé les pilotes ATI, mais ils refusent de s'installer. J'ai contacté le support qui m'a dit ne rien pouvoir faire car cette carte n'est pas destinée aux serveurs. Avez-vous une solution à me proposer?***

R Contrairement à son concurrent Nvidia, AMD/ATI ne produit pas de pilotes pour ses cartes « gamers » installables sur les éditions Windows Server. Il existe cependant une solution hypersimple à mettre en œuvre. Téléchargez les derniers drivers pour « Windows 7 » d'AMD/ATI. Lancez le fichier téléchargé. Celui-ci va décompresser ses fichiers dans un dossier ATI sur le disque C: puis démarrer son installateur. N'allez pas plus loin et quittez-le. Ouvrez le *Gestionnaire de périphériques*. Cliquez du bouton droit sur *Carte graphique VGA standard*. Sélectionnez *Mettre à jour le pilote* et choisissez *Rechercher un pilote sur mon ordinateur*. Cliquez sur *Choisir* parmi une liste de pilotes puis sur *Disque fourni* et pointez vers l'emplacement *C:\ATI\Win7\Packages\Drivers\ Display\W76A_INF* pour désigner le fichier *.INF* qui s'y trouve. Le système affiche alors une liste de cartes. Sélectionnez *ATI Radeon HD 4600 Series*. Le tour est joué ! ■

Release by TEAM-DZ

WINDOWS 7 & SES SECRETS

DÉMARREZ SUR VHD

Q ***Je croyais que l'on pouvait démarrer Windows 7 depuis un disque virtuel VHD, mais je n'ai pas trouvé comment faire...***

R Effectivement, Windows 7 offre la possibilité de démarrer son PC non seulement depuis un disque physique, mais aussi depuis un disque virtuel au format VHD. Il permet de multiplier le nombre de systèmes installés sur sa machine. Pour cela, il faut éditer la configuration du Boot Loader. Si vous êtes expert, la commande en ligne BCDedit permet une telle édition. Sinon, utilisez EasyBCD (www.neosmart.net) et créez une nouvelle entrée en spécifiant le fichier VHD. Une autre solution consiste à utiliser le gestionnaire de démarrage VBoot Menu de VMLite (www.vmlite.com). Il suffit de copier un seul fichier sur l'ordinateur physique, et vous pouvez démarrer des VHD contenant XP, Vista, Linux ou Windows Server ! ■

WINDOWS 7 & LE BUREAU

DES COPIES MAÎTRISÉES

Q ***Par défaut, Windows 7 cherche à copier des fichiers en parallèle lorsque l'on réalise plusieurs copies simultanées. Existe-t-il un moyen pour que les copies soient réalisées en séquentiel ?***

R Supposons que vous fassiez glisser un dossier vers une clé USB. Puis que vous y glissiez un second dossier dans la foulée. Windows va chercher à concrétiser simultanément ces deux copies provoquant un goulot d'étranglement sur la clé et le port USB, ce qui entraîne une chute notable des performances de transfert. D'où l'idée de modifier le comportement de Windows pour qu'il ne réalise plus la copie en parallèle, mais au contraire qu'il enregistre les commandes et les réalise en séquentiel (il copie d'abord le premier dossier et quand cette opération est terminée, il déclenche la seconde). À notre connaissance, il n'existe aucun paramétrage dans la Base de registre pour ajuster ce comportement. En revanche, on trouve sur le marché de petits utilitaires qui remplacent automatiquement et de façon transparente la fonction de copie de Windows, et offre plus de souplesse ainsi qu'une approche séquentielle. Nous pensons notamment à UltraCopier (http://ultracopier.first-world.info) et à TeraCopy (www.codesector.com/teracopy.php). ■

L'ASTUCE À RETENIR

WINDOWS 7

DÉFRAGMENTEZ LE SYSTÈME

Q ***Sous Windows XP, j'utilisais PageDefrag de SysInternals pour optimiser les fichiers système et conserver mes performances. Que puis-je employer de gratuit pour faire de même sous Windows 7 ?***

R Maniaques de la défragmentation, attention ! À trop vouloir défragmenter vos disques avec n'importe quel outil, vous risquez d'obtenir un système moins rapide qu'en laissant Windows 7 s'occuper tout seul de cette problématique. En outre, nous vous rappelons qu'il ne faut pas effectuer cette opération sur les disques SSD. Ces avertissements répétés, il existe effectivement un outil gratuit qui défragmente les fichiers système lors du démarrage, exactement dans le même esprit que l'ancien PageDefrag qui n'est pas compatible Windows 7. Il s'agit de Defraggler 2.x de Piriform (aussi éditeur des célèbres CCleaner et Recuva). À télécharger depuis le site **www.piriform.com**. ■

OFFICE 2010

PLANTAGES WORD

Q ***Sur le nouvel Office 2010 que je viens d'installer, tout fonctionne sauf Word. Il refuse de se lancer. Le problème ne se pose que sur mon profil administrateur. Sur le profil de ma femme, tout fonctionne !***

R Généralement, il suffit d'effacer quelques clés de la Base de registre pour que tout rentre dans l'ordre. Depuis le menu *Démarrer*, lancez *REGEDIT*. Effacez les clés suivantes (ce qui supprimera tout ce qu'elles contiennent) :
** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Data*
** HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Options*
Si ça ne suffit pas, renommez le fichier *Normal.dotm*. Ouvrez l'invite de commandes et saisissez : *ren %userprofile%\Application Data\Microsoft\Templates\Normal.dotm Normal.old*. Si ce n'est toujours pas suffisant, saisissez la commande suivante (toujours depuis l'invite de commandes) : *ren %programfiles%\Microsoft Office\Office14\Startup*.* *.old*. ■

Release by TEAM-DZ

WINDOWS 7 & SES BUGS

RECHERCHE EN PANNE

Q ***Les recherches dans le menu Démarrer ou sur les disques ne fonctionnent plus. C'est très handicapant. Avez-vous une idée de ce qui se passe?***

R Il est probable que le service système qui gère les recherches, Windows Search, ne soit pas actif. Soit parce qu'il a été désactivé par un Spyware ou un logiciel de pseudo-optimisations de Windows, soit parce qu'il rencontre un problème au lancement. Allez dans les outils d'administration et double-cliquez sur *Services*. En bas de la liste, double-cliquez sur *Windows Search*. Vérifiez que le service est bien dans un des modes *Automatique* (dans *Type de démarrage*). S'il n'est pas démarré, cliquez sur le bouton *Démarrer*. Si cela provoque l'affichage d'une erreur, vous êtes face à un bug probablement lié à une corruption des fichiers annexes de Windows Search. Ouvrez l'invite de commandes et saisissez la commande suivante: *DEL C:\Windows\System32\config\TxR*.*/AS*. Redémarrez le PC et attendez que Windows Search reconstruise ses index. ■

WINDOWS 7

LANCEMENT RETARDÉ

Q ***Mon PC met beaucoup de temps à démarrer. En fait, ce délai est principalement lié à toutes sortes d'utilitaires chargés au démarrage et qui restent d'ailleurs visibles dans la zone à côté de l'horloge. Ces outils me sont utiles. Ce que je voudrais, c'est qu'ils se chargent seuls mais pas immédiatement, plutôt quelques minutes après, en tâche de fond.***

R Effectivement, Windows 7 démarre en moins de dix secondes (sur un disque SSD) quand il est vierge de toutes extensions. Ce sont elles, qui gèrent les périphériques et composants spéciaux du PC, qui le ralentissent. Sans compter tous les utilitaires en tâche de fond que nous installons (ou que d'autres programmes Windows installent). Windows 7 a introduit un nouveau concept. Celui de « Services à démarrage retardé ». Il est applicable à la plupart des services Windows. Tapez *Services* dans le menu *Démarrer*, et lancez l'application éponyme. Double-cliquez sur un service lancé automatiquement, et vous découvrirez dans le menu *Type de démarrage* une option *Automatique (début différé)*. Windows Update est un exemple de services configurés par défaut dans ce mode. Symantec, avec son Norton 360 V3, a popularisé l'idée de retarder non seulement le démarrage de services mais aussi celui d'applications et utilitaires exécutés automatiquement au lancement du PC. Heureusement, il n'est pas nécessaire d'effectuer une telle dépense (Norton 360 est l'une des suites les plus complètes, donc les plus chères) pour bénéficier de ce type de fonctionnalité. Startup Delayer 3 de R2 Studios (www.r2.com.au) est un logiciel gratuit et en français, plutôt facile d'emploi. Au lancement, le logiciel récupère la liste des applications placées en démarrage automatique. Il est également possible d'ajouter d'autres applis dont on a quotidiennement besoin, comme par exemple Office Outlook ou Word. Pour chaque application, vous pouvez spécifier, en heure, minute et seconde le délai qui séparera le lancement de l'application du lancement du système… Vous pourrez même préciser si elle doit s'ouvrir normalement, automatiquement, icônifiée en Barre des tâches, ou automatiquement en plein écran. D'autres outils sont capables de retarder le démarrage des programmes, comme LaunchLater de Jeff Cox (http://launchlater.codeplex.com) ou WinPatrol (www.winpatrol.com). ■

WINDOWS 7

BOOSTEZ VOTRE PC

Q ***Faut-il de préférence augmenter la mémoire (j'ai déjà 4 Go) ou opter pour un disque dur SSD afin d'accélérer son PC? Est-ce qu'un SSD est plus utile qu'une clé ReadyBoost. Y a-t-il un intérêt à utiliser deux disques SSD en Raid 0?***

R Plus vous avez de mémoire, mieux c'est pour les applications gourmandes comme la retouche d'images RAW ou le montage vidéo. La mémoire reste aussi essentielle en cas d'utilisation de machines virtuelles. Pour tout le reste, Windows s'exprime à pleine puissance dès que l'on possède 3 Go de Ram. C'est donc au travers de l'adoption d'un disque SSD (sur lequel vous installerez Windows et ses applications) que les améliorations en termes de performances peuvent se réaliser. Vous découvrirez alors un système qui démarre en moins de dix secondes, des applications qui s'ouvrent instantanément et des machines virtuelles qui bootent en cinq secondes. Le remplacement du disque dur par un disque SSD fait une très grosse différence. C'est vraiment l'un des meilleurs moyens de booster son PC, même si le coût de tels disques demeure encore élevé. Le gain est instantanément perceptible contrairement à ReadyBoost qui n'accélère que le chargement de certaines applications. De toute façon, Windows 7 désactive ReadyBoost lorsqu'il détecte qu'un disque SSD est connecté au système. Par contre, contentez-vous d'un seul disque SSD, car la commande TRIM (qui permet des performances optimales sur SSD) ne fonctionne pas sur les configurations en Raid 0. ■

Release by TEAM-DZ

LES CHAÎNES DU WEB

UN WEB TUNER POUR WEB TV…

Q ***Avec toutes les chaînes de télévision aujourd'hui sur internet, y a-t-il moyen de regarder la télé sur Windows Media Center sans y ajouter de tuner ?***

R Il existe différentes solutions. Tout d'abord, la section TV de Media Center possède une chaîne « TV différée », fort mal nommée, qui propose les contenus de MSN Vidéo. Ensuite, l'extension TunerFree MCE de MillieSoft s'insère dans le menu principal de Media Center et offre un accès immédiat. Autre option, « SecondRunTV 3.0 » (moins de 5 €) donne en théorie accès à toutes les chaînes de télé diffusées via le web. En pratique, le logiciel n'est préconfiguré que pour les programmes américains et nécessite un peu d'expertise pour être étendu aux chaînes françaises. ■

TUNER TNT RÉSEAU

POUR PARTAGER LA TÉLÉ

Q ***Comment puis-je faire en sorte que tous mes PC sous Windows 7 accèdent à la TV TNT sans ajouter à chacun d'eux un tuner TNT, car je n'ai qu'une seule prise antenne hertzienne dans la maison et pas de réception avec une antenne intérieure ?***

R Deux solutions sont possibles. La première consiste à équiper un de vos ordinateurs d'une carte tuner compatible (on en trouve chez Hauppauge et chez Terratec) avec le logiciel DVBLink Server Network Pack (www.dvblogic.com). La seconde solution est d'opter pour le boîtier EyeTV Netstream DTT (www.elgato.com). Celui-ci comporte deux tuners TNT. On le branche directement à l'antenne hertzienne ainsi qu'au réseau local grâce à sa prise ethernet. Tous les PC du foyer peuvent alors accéder à ce boîtier et deux émissions différentes peuvent être regardées/enregistrées simultanément. Il suffit simplement d'installer le pilote Windows Media Center livré sur chacune des machines. EyeTV NetStream DTT est également fourni avec un logiciel qui permet de regarder la télévision sur les PC sans pour autant utiliser Media Center. Enfin, EyeTV possède aussi un client iPad pour regarder les chaînes depuis sa tablette Apple ! ■

L'ASTUCE À RETENIR

CONFIGURATION AVANCÉE

DES LOGOS ET DES CHAÎNES

Q ***Est-il possible d'afficher les logos des chaînes plutôt que leur nom ? Dans l'affirmative, comment procéder ?***

R Il est effectivement possible d'afficher les logos des chaînes mais à côté de leur nom plutôt qu'en remplacement. L'opération nécessite un peu de patience et beaucoup de manipulations car elle n'a rien d'automatique. Pour la réaliser, il faut commencer par télécharger un petit utilitaire dénommé My Channel Logos (**http://mychannellogos.com/dl.aspx**). Celui-ci existe en deux versions : une pour les éditions 32 bits et une pour les éditions 64 bits. Vous devez préalablement avoir déjà installé un tuner sous Windows Media Center et réalisé intégralement le processus d'installation des chaînes. Ces opérations préliminaires réalisées, quittez Media Center et lancez *My Channel Logos*. Celui-ci récupère la liste des chaînes détectées par Media Center et l'affiche sous forme arborescente. Cliquez sur une chaîne dans la liste, puis diquez sur la zone vierge du logo. Choisissez un fichier PNG contenant le logo de la chaîne (que vous aurez préalablement récupéré sur le web en faisant une recherche d'images sous Bing ou Google). Répétez l'opération pour chaque chaîne. Le logiciel convertit automatiquement l'image fournie dans un format PNG (96 x 42 pixels) qui gère les transparences. ■

AJUSTEMENT

DES PAUSES PLUS LONGUES

Q ***Pouvez-vous m'indiquer comment ajuster la durée du buffer de pause sous Windows Media Center ?***

R Windows Media Center transforme votre PC en véritable enregistreur numérique avec toutes les fonctions traditionnelles de ce type d'appareil, telles que la mise en pause du direct. En fait, dès que vous regardez une émission, celle-ci est automatiquement enregistrée dans un buffer. Cela permet de revenir en arrière pour revoir une action ou de mettre en pause le direct. La taille de ce buffer est définie par une clé en Base de registre. Lancez *Regedit* et déployez la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Media Center\Service\Video\Tuners\DVR*. Repérez la clé BackingStoreEachFileDurationSeconds, cliquez sur *Décimale* et entrez le nombre de secondes mémorisées par le buffer. Par défaut, Media Center alloue 300 secondes, autrement dit cinq minutes. Doublez cette valeur. ■

Release by TEAM-DZ

OPTIONS DE PAGE

UN EPG HAUT EN COULEUR

Q ***Je trouve le guide électronique des programmes de Windows Media Center bien triste comparé à ceux que l'on trouve sur les TV TNT actuelles. N'y a-t-il donc aucun moyen de colorer les programmes en fonction de leurs types ? Ou de les trier par types ?***

R Mais si, c'est possible. Et il n'y a même pas besoin de tricher pour ça ! C'est un des paramétrages disponibles en standard. Allez dans *Tâches*, dans *Paramètres* puis dans *TV*, et enfin dans *Options de page du Guide*. Cochez alors la case *Applique aux émissions des arrière-plans en couleur en fonction de leur catégorie*. Cliquez sur *Enregistrer* et revenez au Guide des programmes pour admirer les changements… Quant au tri par catégorie, il n'est pas en soit possible mais on peut en revanche filtrer l'affichage pour n'afficher que les émissions d'une catégorie. Il suffit pour cela de déployer le panneau *Afficher les catégories* situé à l'extrême gauche du guide. ■

PRÉSENTATION

CONTRÔLEZ LE DÉMARRAGE

Q ***La petite présentation d'introduction de Windows Media Center est certes très jolie mais à la longue, elle finit par se montrer gênante car elle retarde l'accès aux fonctionnalités réelles ; ce qui est handicapant quand on veut enregistrer une émission dans l'urgence. Peut-on la supprimer ?***

R C'est en effet possible. Comme nombre d'applications Windows, Media Center utilise des « switches » (des paramètres en ligne de commande) pour influencer son comportement au démarrage. Ouvrez le menu *Démarrer*, cliquez du bouton droit sur *Windows Media Center* et sélectionnez *Propriétés*. Dans l'onglet *Raccourci*, repérez le champ Cible (il contient la valeur *%windir%\ehome\ehshell.exe*). Sans effacer le champ, placez le curseur à la fin, ajoutez un espace, puis saisissez le paramètre « */nostartupanimation* ». Cliquez sur *OK*. Windows Media Center propose bien d'autres switches que vous pourrez utiliser de la même manière que /nostartupanimation et même parfois combiner ensembles. Voici la liste de ces switches : « /noshutdownui » supprime la fonction *Éteindre* qui apparaît dans le menu *Tâche*. « /widescreen » force l'affichage en mode 16:9, même sur un écran 4:3 lorsque Media Center est en mode fenêtre. « /screensaver » démarre automatiquement Media Center dans son mode écran de veille. « /configuress » lance directement Media Center sur son écran de paramétrage de l'écran de veille. « /playslideshowwithmusic » démarre automatiquement Media Center en mode diaporama avec musique. « /playfavmusic » démarre systématiquement Media Center en mode lecture de vos musiques favorites. « /playallmusic » fait la même chose en prenant en compte toutes les musiques. « /nochrome » incruste Media Center à l'écran sans pour autant afficher les contours de la fenêtre : ce qui interdit son déplacement ou l'ajustement de sa taille. « /mediamode » force l'affichage de Media Center en mode plein écran sans possibilité de repasser en mode fenêtre, ni possibilité de fermer Media Center autrement qu'en fermant la session ou le PC. Revient à un mode kiosque. « /directmedia:general » affiche Media Center en plein écran sans pour autant le figer dans ce mode (contrairement à /mediamode). « /directmedia:tv » lance Media Center directement sur le mode TV en direct. « /directmedia:video » lance automatiquement Media Center sur son écran d'affichage de sélection des vidéos. ■

MEDIA CENTER ET LES APPLICATIONS WINDOWS

ENRICHISSEZ MEDIA CENTER

Q ***Peut-on intégrer ses propres applis dans l'interface Media Center ? Je voudrais pouvoir accéder à d'autres applications Windows plein écran depuis l'interface Media Center du PC connecté à ma TV. Je pense notamment à Zune Player (j'ai un Windows Phone 7).***

R La solution la plus simple pour intégrer des applications classiques dans les menus de Windows Media Center consiste à télécharger et lancer le programme Media Center Studio (http://adventmediacenter.com). Ce logiciel permet de personnaliser les menus de l'interface Media Center. Ouvrez l'onglet *Start Menu*, cliquez sur *Application* et indiquez le chemin d'accès au fichier *Zune.exe* dans le champ *Path*. Précisez que le logiciel aura accès aux fonctionnalités Audio, DirectX, Intense Rendering et Vidéo. Sélectionnez *Stop the currently playing media* dans le menu *popup*. Retournez dans l'onglet *Home* et cliquez sur *Save*. Activez la fenêtre *Start Menu* et déployez le panneau inférieur *Entry Points*. Faites glisser l'icône Zune nouvellement créée vers l'emplacement désiré sur l'interface Media Center. Cliquez sur *Save*. Lancez *Windows Media Center* et vérifiez que l'icône Zune a bien fait son apparition. Vous pouvez réaliser le même genre d'intégration avec n'importe quel logiciel Windows. ■

Release by TEAM-DZ

WINDOWS & SP 1

REFUS D'INSTALLATION

Q ***Pendant l'installation du SP1, Windows affiche l'erreur « L'installation du Service Pack ne peut continuer ». Que faire ?***

R Plusieurs raisons peuvent entraîner l'apparition de cette erreur. Toutefois, il semble que la principale cause de cette erreur soit la présence d'une version trop ancienne de Microsoft Security Essentials sur votre PC. Commencez donc par désinstaller cette version caduque. Installez ensuite le SP1. Puis allez sur le site valide. Téléchargez la dernière version en date de l'antivirus gratuit de Microsoft. D'une manière générale, les antivirus et autres outils de sécurité sont une cause classique d'échec d'installation du SP1. Pensez à les désactiver. ■

SP1 & ÉCRAN BLEU

RESTAUREZ LE SYSTÈME

Q ***J'ai installé le SP1. Malheureusement au redémarrage j'obtiens un écran bleu avec l'erreur C000009A. Je ne sais vraiment pas quoi faire.***

R Espérons pour vous que vous n'aviez pas désactivé la fonctionnalité *Restauration du système* de Windows 7… car vous allez en avoir besoin ! Cette erreur est en effet provoquée par les packs linguistiques disponibles sur les versions Entreprise et Ultimate. Il vous faut d'abord reprendre la main sur Windows. Redémarrez votre PC en appuyant sur la touche [F8] Lorsque l'écran des options avancées de démarrage apparaît, sélectionnez *Réparer l'ordinateur*. Lorsque l'ordinateur vous propose la boîte de dialogue *Options de récupération système*, sélectionnez *Restaurer le système*. Choisissez un point de restauration antérieur à l'installation du SP1. Laissez le système se réparer et redémarrer automatiquement. Une fois de retour sur le bureau Windows, il faut remédier à la cause de l'erreur. Allez dans le panneau de configuration et dans le champ de recherche saisissez « langue ». Cliquez sur *Installer ou désinstaller les langues d'affichage*. Cliquez sur *Désinstaller des langues d'affichage*. Cochez toutes les langues (sauf celle active), puis cliquez sur *Suivant*. Après le redémarrage de Windows, relancez l'installation du SP1. ■

L'ASTUCE À RETENIR

SP1 & OCCUPATION DISQUE

FAITES DE LA PLACE

Q ***Depuis que j'ai installé le SP1, mon espace libre s'est redoutablement réduit sur mon disque système, qui se trouve être un disque SSD à l'espace pour le moins précieux. D'où provient ce superflu ? Peut-on l'éliminer ? Comment récupérer de la place sans mettre en péril l'installation ?***

R Entre ses fichiers temporaires et les sauvegardes permettant un retour en arrière, l'installation du Service Pack 1 se révèle très gourmande en espace disque. Heureusement, il est possible de récupérer l'espace disque perdu très simplement. Toutefois, avant de vous lancer dans cette opération de nettoyage, attendez quelques jours pour vérifier que toute votre configuration fonctionne à merveille sous SP1. Si tout est parfaitement opérationnel, vous n'aurez pas besoin de désinstaller le SP1 et vous pouvez donc en supprimer les fichiers de sauvegarde. Faites donc de la place en lançant « cleanmgr » depuis le menu *Démarrer*. Sélectionnez le lecteur C, puis cliquez sur *Nettoyer les fichiers système*. Une liste étendue de fonctions s'affiche alors. Cochez *Fichiers de sauvegarde du Service Pack*. Cliquez sur *OK*. Et rappelez-vous qu'il sera impossible de désinstaller le SP1 après cette opération de nettoyage ! ■

SP1 & RC

DÉSINSTALLEZ LE SP1

Q ***Peut-on désinstaller le SP1 ? En fait j'avais installé le SP1 Release Candidate. Mais la version finale du SP1 ne peut s'installer par-dessus. Il me faut donc préalablement désinstaller la RC…***

R Il faut effectivement désinstaller la « Release Candidate » préalablement à l'installation de la version finale du SP1. Normalement, il faut suivre la procédure suivante : Allez dans le Panneau de configuration. Cliquez sur *Programmes*, puis *Afficher les mises à jour installées*. Cochez *Service Pack pour Microsoft Windows (KB 976932)*, puis cliquez sur *Désinstaller*. C'est la méthode officielle pour désinstaller le Service Pack 1, y compris dans sa version finale. Toutefois, cette désinstallation n'est possible que si vous n'avez pas supprimé les fichiers de sauvegarde associés. Si les fichiers ont été supprimés, vous devrez malheureusement réinstaller Windows 7 (éventuellement en faisant une sorte de réparation via l'installation en mode « mise à jour »). ■

Release by TEAM-DZ

WINDOWS UPDATE & SP1

BLOQUEZ L'INSTALLATION DU SP1

Q ***Avant d'installer le SP1 sur tous mes PC, je souhaiterais attendre un peu et vérifier que les utilisateurs ne rencontrent aucun problème avec les applications que j'utilise, notamment pour mon travail. Peut-on bloquer l'installation automatique du SP1 sur les machines ?***

R Si vous voulez bloquer l'installation automatique du SP1 sur vos PC par Windows Update, Microsoft propose un petit utilitaire à télécharger, dénommé SPBlockerToolkit. Vous pouvez le télécharger depuis le centre de téléchargement du site de Microsoft ou depuis l'URL suivante : http://bit.ly/f0PL50. Cet utilitaire modifie en réalité une clé en Registry *HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate*. Cette clé contient une valeur dénommée « DoNotAllowSP ». Si vous placez cette valeur à 1, l'installation du Service Pack sera bloquée (jusqu'à ce que vous replaciez cette valeur à 0).■

SP1 & .NET

PROBLÈMES DE PERFORMANCE

Q ***Depuis que j'ai installé le SP1 de Windows 7, ma machine rame terriblement. J'ai passé deux CD Antivirus de Scan (Kaspersky et GData) et ils n'ont rien trouvé. Je n'ai pas l'impression que le problème soit lié à une infection mais vraiment au SP1.***

R Il existe une cause reconnue de ralentissement du SP1. Appuyez sur [CTRL]+ [ALT]+ [ESC] pour appeler le gestionnaire de tâches. Cliquez ensuite sur le bouton *Afficher les processus de tous les utilisateurs* pour obtenir la liste complète des programmes en cours d'exécution. Cliquez sur l'en-tête de la colonne *Processeur* afin de classer les applications par consommation machine (du plus consommateur au moins consommateur). Regardez si une application (autre que « Processus inactif du système ») occupe plus de 40 % du temps machine. Si cette application se nomme « mscorsvw.exe », vous êtes dans le cas connu de ralentissement. Sinon, c'est peut-être une application incompatible : regardez à quel logiciel appartient ce processus, essayez d'obtenir une mise à jour après de l'éditeur ou tentez simplement sa désinstallation/réinstallation.

Mais revenons au cas « mscorsvw ». Cette application se charge en réalité de précompiler les programmes « .NET » en code natif afin d'en accélérer l'exécution. Certains éléments du SP1 s'appuient en effet sur le .NET Framework. Pour qu'ils s'exécutent plus rapidement, Windows doit les recompiler en utilisant les informations d'encodage propres à votre PC. Ce processus est totalement automatisé et nécessite normalement une dizaine de minutes. Il n'est lancé que lorsque Windows détecte une période d'inactivité. Mais votre antivirus ou un souci annexe peuvent empêcher ou ralentir son bon fonctionnement. Débranchez votre PC du réseau (pour éviter tout risque). Éteignez votre antivirus. Déployez le menu *Démarrer* et dans le champ de recherches, saisissez CMD et validez en appuyant sur [CTRL] + [SHIFT] + [ENTREE] afin d'exécuter l'invite de commandes en mode administrateur. Puis saisissez les deux commandes suivantes (en validant chaque ligne par la touche [Entrée]) :

CD C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727

NGEN executequeueditems

Une fois la commande terminée, fermez l'invite de commandes et redémarrez le PC. ■

SP1 & SES BUGS

ERREUR 490 AU DÉMARRAGE

Q ***Depuis ce matin, impossible de redémarrer le PC. L'image s'affiche, le BIOS se lance normalement, mais quand Windows essaye de se charger j'obtiens une erreur 0x490. Que faire ?***

R Il peut arriver après une panne de courant, mais aussi suite à une défaillance matérielle, une installation défaillante du SP1 ou un virus, que l'ordinateur ne puisse redémarrer et affiche alors l'erreur 0x490. Cette erreur traduit une panne au niveau du Gestionnaire de démarrage (le Boot Manager) le plus souvent provoqué par un souci au niveau du MBR (Master Boot Record) ou des fichiers de lancement de Windows. Redémarrez le PC depuis le DVD de Windows 7 (ou depuis le CD/DVD de réparation généré depuis l'option *Créer un disque de réparation système de Windows 7*). Si vous ne disposez pas d'un tel CD, utilisez le PC d'un ami pour le générer et/ou le télécharger (cherchez Windows 7 System Recovery Disk sous Google/Bing). Appuyez sur une touche lorsque le boot vous le demande. Lorsque le premier écran d'installation apparaît, cliquez sur le lien *Repair your Computer* ou *Réparer l'ordinateur*. Sélectionnez à l'installation la partition Windows 7, cliquez sur *Next/Suivant* puis sur *Startup Repair* (ou *Réparation du démarrage*). Laissez l'assistant réaliser la réparation. Puis redémarrez le PC après avoir retiré le DVD. ■

Release by TEAM-DZ

WINDOWS 7 ET BLUETOOTH

BUGS BIZARRES EN BLUETOOTH

Q ***J'utilise Windows 7 en version 64 bits. Les pilotes semblent être bien installés, mais je n'arrive pas à accéder à la liste des appareils Bluetooth. Que dois-je faire ?***

R Si le service de Bluetooth refuse de démarrer au lancement de Windows ou si l'opération de recherche des périphériques Bluetooth, lancée depuis le Panneau de configuration, part dans une boucle sans fin, vous êtes victime d'un bug identifié de Windows 7 sur la couche Plug and Play. Heureusement, il existe un correctif à ce problème. Malheureusement, celui-ci n'est pas encore disponible à tous. Il faut passer par le support Microsoft et demander le Fix308817. Ce correctif correspond à l'article 980396 de la base de connaissance de Microsoft (http://support.microsoft.com/kb/980396/). ■

IE8 ET LA SÉCURITÉ

EXTENSIONS INTERDITES

Q ***Je suis devenu particulièrement paranoïaque en matière de sécurité sur le web. Y a-t-il un moyen d'éviter qu'Internet Explorer utilise les extensions propres à Microsoft ?***

R Les extensions sont quasi indispensables aujourd'hui. Leur présence a assuré en grande partie le succès de Firefox. Et leur absence a longtemps pénalisé Google Chrome qui connaît un regain d'intérêt depuis l'arrivée des extensions sur sa version 4. Mais il est vrai qu'elles représentent aussi une menace potentielle. Il existe effectivement un moyen de brider IE8 dans son usage des extensions : ouvrez le menu *Outils*, allez dans *Options Internet*, ouvrez l'onglet *Avancé*, balayez la liste des paramètres jusqu'à la section Navigation et décochez la case *Activer les extensions tierce partie du navigateur*. Validez par *OK* puis relancez le navigateur. Notez que cette option, destinée à renforcer la sécurité du navigateur, reste différente de la fonction *Internet Explorer* (sans modules complémentaires) du menu *Démarrer* qui, elle, est plutôt destinée à des fins de maintenance et d'analyse d'erreur. Car, rappelons que la première cause de bug de IE8 est la présence d'extensions et modules complémentaires peu fiables au cœur du navigateur. Vous pouvez les lister et les désactiver manuellement en passant par la fonction *Gérer les modules complémentaires* du menu *Outils*. ■

L'ASTUCE À RETENIR

WINDOWS 7 ET SA TASKBAR

RACCOURCI POUR CACHER LA BARRE DES TÂCHES

Q ***J'utilise un netbook sous Windows 7. Comme la résolution graphique est relativement restreinte, j'utilise la fonction*** **Cacher automatiquement la Barre des tâches** ***afin de récupérer un peu d'espace. Mais je ne la trouve pas très pratique, certaines manipulations de la souris ayant tendance à la faire réapparaître intempestivement. Une solution ?***

R Tout d'abord, n'oubliez pas que l'on peut ajuster la position de la Barre des tâches. Ainsi sur les écrans larges des netbooks, il est souvent plus agréable de l'afficher sur le côté de l'écran : cliquez du bouton droit sur une zone vierge de la Barre des tâches, choisissez *Propriétés*, et dans le menu Position de la Barre des tâches, sélectionnez *À droite*. Ensuite, il existe un petit utilitaire gratuit qui permet de contrôler manuellement l'apparition/disparition de la Barre des tâches. Il suffit de l'installer dans le dossier Démarrage de Windows, puis d'utiliser la combinaison de touches [CTRL] + [ESC] pour alternativement cacher ou afficher la Taskbar de Windows. Créée par Ritesh Kawadkar du Windows Club, Hide Taskbar 1.0 peut être téléchargée à cette URL :
www.thewindowsclub.com/downloads/Hide-Taskbar.zip ■

WINDOWS 7 ET LES PROFILS

L'EMPLACEMENT DE L'UTILISATEUR

Q ***Je voudrais déplacer tous les dossiers de mon profil utilisateur (mes documents, mes favoris, mon bureau, etc.) sur le disque D: au lieu du disque C: afin de pouvoir réinstaller le système à volonté, sans avoir à sauvegarder/restaurer mes données. Une solution simple ?***

R Il est possible de déplacer les dossiers du profil utilisateur soit simplement en réalisant un déplacement à la souris depuis le bureau, soit en passant par les propriétés de ces dossiers et l'onglet *Emplacement*. Malheureusement, l'opération doit être réalisée manuellement pour chaque dossier. Un processus long et fastidieux. Il existe une autre solution qui, en un clic, déplace tout le profil. Profile Relocator est un utilitaire gratuit dédié à ce déplacement. Mais attention, pour éviter tout dysfonctionnement avec les applications installées, il n'est pas applicable aux profils existants mais uniquement à tout nouveau profil créé (http://software.bootblock.co.uk/?id=profilerelocator). ■

Release by TEAM-DZ

WINDOWS 7 ET LA VIDÉO

RÉALISEZ LA ROTATION D'UNE VIDÉO

Q ***Comment réaliser la rotation à 90° d'une vidéo tournée en mode portrait sous Windows 7?***

R Plusieurs solutions à cette question qui revient fréquemment. Tout d'abord, si vous utilisez le lecteur multimédia VLC Media Player, vous pouvez aisément réaliser une rotation: Appuyez sur [CTRL] + [E] lors de la lecture de la vidéo, allez dans l'onglet *Effets Vidéo*, cochez *Transformation* et sélectionnez la rotation désirée. De même, si vous montez des vidéos sous Windows Live Movie Maker, l'opération se réalise en un clic: une fois la vidéo importée, allez dans l'onglet *Accueil* et diquez sur les icônes de rotation dans la section *Édition*. Enfin, il existe différents utilitaires capables de redresser une vidéo. La solution la plus facile à mettre en œuvre est sans aucun doute le petit outil gratuit et en français de DVDVideoSoft: Free Video Flip and Rotate. Très simple et compatible avec de nombreux formats. (www.dvdvideosoft.com/products/dvd/Free-Video-Flip-and-Rotate.htm). ■

WINDOWS 7 ET READYBOOST

COUP DE BOOST POUR VOS NETBOOKS

Q ***Depuis que j'ai installé Windows 7 sur mon netbook, je réalise que je l'utilise chaque jour davantage et lui demande désormais des opérations qui sont à la limite de sa portée, notamment en raison de sa mémoire RAM limitée à 1 Go. J'envisage de passer la mémoire à 2 Go qui est le maximum supporté par ce PC. Auriez-vous une autre idée?***

R Booster la mémoire à 2 Go est en effet votre première urgence. Mais même ainsi, cela risque de n'être pas suffisant pour une utilisation intensive. C'est dans ce genre de situation que l'on apprécie une fonction méconnue et mal-aimée de Windows Vista et Windows 7: ReadyBoost. Cette fonction a été grandement améliorée sous Windows 7 et procure un réel bénéfice lorsque la mémoire RAM est restreinte. ReadyBoost ne fait pas de miracle, mais ajoute un mieux notable en matière de confort d'utilisation. Avec W7, vous n'êtes plus limité à l'usage de clés USB. La fonction est désormais disponible en utilisant des cartes SD. Un choix judicieux sur un netbook, car on peut ainsi facilement laisser la carte dans le lecteur sans qu'elle dépasse ou nuise à la mobilité de l'appareil. Veillez toutefois à acquérir une de ces SD « hautes performances », certes plus chères mais indispensables à un fonctionnement optimal de ReadyBoost. Une fois la carte SD ou la clé USB installée et validée pour un usage ReadyBoost, vous devriez constater des gains très sensibles, notamment dans l'ouverture des applications ou dans la réactivité du clic droit sous l'explorateur, par exemple. N'hésitez pas à opter pour une carte de 4 Go ou même mieux de 8 Go. Et dédiez-la intégralement à Windows 7. Signalons également que si sous Vista, ReadyBoost était limitée à une seule clé de 4 Go maximum, sous W7 ReadyBoost peut être réparti sur huit périphériques et supporte jusqu'à 32 Go… Vous pouvez surveiller l'activité et l'efficacité de ReadyBoost soit en utilisant l'analyseur de performances de Windows 7 – vous trouverez différents compteurs dans la section Cache ReadyBoost – soit à l'aide de l'utilitaire Ready Boost Monitor de URG Systems. (www.urgsystems.com/products/ready-boost-monitor.aspx). ■

WINDOWS 7 ET FIX IT

RÉPARATEUR TRÈS PERFORMANT

Q ***Quand je rencontre des problèmes bizarres de fonctionnement sur Windows XP, j'utilise l'outil Dial-A-Fix de DjLizard. Existe-t'il une trousse de réparation similaire pour Windows 7?***

R Dial-A-Fix est un outil aujourd'hui à l'abandon. Mais il existe bien une super-trousse de réparation pour Windows 7… produite par Microsoft! Il s'agit d'un tout nouvel outil gratuit, à installer d'urgence sur tous les PC sous W7. Fix It Center est l'outil qui manquait à Windows. Le logiciel regroupe toutes les fonctions de réparation inventées par le support technique de l'éditeur. Le logiciel s'actualise automatiquement via internet et s'enrichit donc semaine après semaine. Il comporte déjà près d'une trentaine de fonctions de réparation pour vos problèmes de connexion internet, de dossiers partagés, de lecture DVD, de groupe résidentiel, de performances, de tuner TV, de bibliothèque multimédia et Media Player, de plantages d'IE8, de sécurité, d'alimentation, de compatibilité, de Windows Update, d'affichage Aero, etc. Fix-It Center (fixitcenter.support.microsoft.com) se révèle très convivial et pratique. N'hésitez pas à le sortir à la moindre difficulté. Les corrections sont totalement automatisées et elles n'ont aucun impact si vous essayez d'en lancer une alors que tout va bien. Vous y trouverez non seulement des outils de réparation, mais aussi quelques outils de maintenance bienvenus. ■

Release by TEAM-DZ

GUIDE DE SÉCURITÉ POUR VOTRE PME

Courtisées par les vendeurs d'outils de sécurité, les PME doivent recenser les problématiques auxquelles elles sont confrontées. **Les choix s'avèrent souvent basés sur un compromis**. Mais les promesses charmeuses de solution « complètes » peuvent cacher souvent de sérieuses lacunes.

SOMMAIRE

LA PROTECTION DU « PÉRIMÈTRE »
Déterminer les objets à protéger n'est pas toujours facile.

L'UTM, LE COUTEAU SUISSE DE LA PROTECTION
Le tout en un réclame une maintenance non négligeable.

L'IDS-IPS, UN CHIEN DE GARDE DIFFICILE À DRESSER
Régler les appareils nécessite une formation ou un support technique.

La protection des petites PME et des TPE est un problème quasiment insoluble : à la fois proche techniquement des besoins éprouvés par les utilisateurs de réseaux familiaux, mais également comparables aux attentes des grandes entreprises pour des raisons tant règlementaires qu'économiques. Tant que les menaces se limitaient, jusqu'à la fin des années quatre-vingt-dix, à quelques virus et tentatives d'intrusion, le couple antivirus/firewall suffisait amplement. D'ailleurs, les éditeurs ont tellement ressassé cette rengaine qu'il est encore difficile de nos jours de convaincre certains chefs d'entreprise d'acquérir une nouvelle génération de boucliers numériques (VPN, firewall d'applications web…). Inertie d'autant plus compréhensible que les menaces évoluent (le « bon vieux virus » ne représente qu'une part infime des risques visant les entreprises) et que toutes les menaces ne visent pas de manière égale les consommateurs.
La part exagérée du risque « perte d'information » et l'accent mis sur les DLP (outils de prévention de fuites d'information) concernera peu un industriel du secteur sidérurgique, pour qui l'infection par un virus du réseau gérant les automates et la régulation sera prioritaire. Le DLP intéressera un peu plus un collectif de médecins manipulant des informations personnelles confidentielles (dossiers médicaux notamment) ou une entreprise d'ingénierie dont les « avoirs » sont essentiellement constitués de secrets de fabrication. Il n'y a donc pas de prêt-à-porter sécurité PME/TPE. Paradoxalement, cette uniformité des mécanismes de protection commence à jouer dans le cadre d'entreprise de moyenne et grande envergure, qui utilisent des modèles organisationnels précis et reproductibles.

Des petites entreprises plus vulnérables

Par ailleurs, les cybermenaces évoluent proportionnellement à l'accroissement du nombre d'usagers du réseau internet. Si la proportion « gentils-méchants » est généralement stable, l'augmentation en volume et en diversité est très nette depuis ces cinq dernières années. D'autant plus nette que ce sont les ordinateurs familiaux et les grandes entreprises qui ont fait les frais des premiers assauts des cybermafias… et qui se sont protégés en conséquence.
Face au durcissement des carapaces numériques, les techno-délinquants se rabattent sur l'industrie : les petites entreprises, généralement mal protégées, ne disposant que très rarement de budget de protection reconductible d'une année sur l'autre… et surtout capable de savoir « là ou çà fait mal ». Si, dans 90 % des grandes entreprises, les « avoirs » (propriété

Release by TEAM-DZ

intellectuelle, richesses commerciales, secrets de fabrication, fichiers clients, contrats fournisseurs…) sont connus et maîtrisés, il est fréquent qu'un patron de PME soit totalement incapable de situer exactement quels sont ses richesses (c'est souvent plus son fichier client que ses méthodes de production) et encore moins à même de dire à quel endroit lesdites richesses sont accessibles : sur quel ordinateur, sur quel réseau, sur quel disque dur amovible, voir sur quel appareil mobile. Avant d'acheter un « machin informatique à protéger », la première question que doit se poser un entrepreneur est « qu'est-ce que je dois protéger ? ». Et, témoignent bien souvent les « auditeurs » en sécurité, bien rares sont ceux qui le peuvent véritablement.

Dossier réalisé par Marc Olanié et Solange Belkhayat

Focus | La protection du périmètre

COMMENT SE PROTÉGER QUAND ON EST UNE PME? Renaud Bidou, Expert en sécurité chez DenyAll, s'est penché sur la question de la protection des sociétés de moindre envergure, ***« Généralement dans les petites structures, il n'y a pas d'expert en sécurité donc quel que soit l'équipement, il faut qu'il fournisse un niveau de sécurité suffisant et ce, de façon très simple. Le second point à ne pas sous-estimer est le nombre d'équipements à mettre en place. Une solution de DLP, un firewall, un IDS et/ou un IPS … même si les équipements sont abordables en termes d'utilisation, cela devient tout de même ingérable. La problématique est identique si l'on considère le cloud et la sécurité via le cloud. Il permet de ne pas avoir à gérer en interne l'infrastructure, néanmoins il va quand même falloir le configurer et gérer le contrat de services derrière. La principale difficulté sera de savoir ce que l'on veut protéger. Une PME qui n'a qu'un serveur web pourra envisager une solution avec un WAF, Web Application Firewall, très simple à mettre en œuvre, et également du partage de fichiers, un DNS… Elle pourra peut-être s'orienter vers une solution IDS ou IPS. Mais attention, il y a beaucoup de remontées d'informations dans le cas d'une solution IDS, d'alertes qu'il faut creuser, et donc l'IPS est beaucoup utile dans le cadre d'une PME car en plus de détecter, il réagit. Concernant le firewalling en PME, il existe des solutions telle celle d'Astaro, qui propose l'UTM avec la fonction pare-feu. Il s'agit d'un produit facile à manipuler et que tout le monde peut maîtriser. »***

Release by TEAM-DZ

l'UTM ou l'antitout plug & play

Présentés comme la panacée de la protection, les UTM sont avant tout un patchwork d'outils de sécurité « moyennement bien adaptés » aux demandes des PME. Souvent comparés au couteau suisse de la sécurité, ils sont incontournables.

Le sigle ne s'est réellement répandu que vers la fin 2005 : UTM, pour « Unified Threat Management », en français « gestion centralisée des menaces ». Son apparition correspond à l'arrivée en masse de l'ADSL aux USA (en net retard par rapport à l'Europe), ouvrant la porte du « net » aux TPE américaines. Il s'agit là d'un marché que ne savaient pas couvrir les professionnels de la protection « périmétrique » traditionnelle, comme les McAfee, les Symantec, les ISS ou les Cisco. Car cette clientèle d'agences ou de professions libérales, qui possède entre deux et dix ordinateurs, ne peut se contenter d'une « suite logicielle » traditionnelle conçue pour les postes de travail, et n'accepte pas de payer le prix fort d'un gros firewall, d'un IDS, d'un routeur et d'une passerelle VPN conçus pour le débit d'une grosse entreprise. Timidement apparaissent quelques productions « made in Taiwan », constituées d'un ordinateur minimaliste, et d'un ensemble logiciel pré-installé : coupe-feu, IPS, VPN, antivirus, antispam, antiphishing… il ne faudra pas longtemps pour que, du stade de bidouille, l'UTM devienne un véritable équipement intégré, s'intercalant entre la prise « internet » et le réseau local, et équipé d'une seule commande : un bouton marche-arrêt. C'est là une vision caricaturale, mais pourtant assez juste. Car le principal crédo des vendeurs d'UTM se résume au slogan « simple et pas cher ».

Quid des qualités et défauts des UTM ?

Les UTM sont-ils parfaits ? loin s'en faut… un bon hacker peut contourner bon nombre d'entre eux… mais c'est également le cas d'appareils plus haut de gamme. Sont-ce là de simples intégrations logicielles dans un boîtier ? Pas seulement car (voir l'encadré ci-contre) ils possèdent des agents et mécanismes d'administration, des extensions de gestion des communications avec les postes mobiles situés en dehors du périmètre (VPN-SSL) que l'on voit très rarement dans les suites logicielles. En outre, le fait qu'ils concentrent, en un « point de passage obligé », toutes les fonctions de protection périmétrique ainsi que, pour certains, d'extension VoIP et d'un routeur /commutateur (pour mieux gérer les segmentations réseau et les constitutions de DMZ) font totalement oublier le côté désagréable de l'UTM : l'abonnement de mise à niveau, « l'impôt » de mise à jour antivirus, antispam, règles de firewall, etc. Cette « dime de la sécurité », si elle est totalement admise au sein des grandes entreprises, passe avec plus de difficultés dans les TPE. Ce n'est pas un hasard si Microsoft a abandonné le modèle payant des clients « forefront » (alias l'antivirus

Achat | Trois boîtiers UTM

> Fortigate-60C, Fortinet

Ce boîtier propose une protection multimenaces grâce à la présence d'un pare-feu, d'IPSec et d'un VPN SSL, d'un antivirus, d'un antispam, d'un IPS et enfin des fonctions de filtrage web. En plus, il est possible de prévenir la perte de données grâce à un dispositif DLP, de faire du contrôle d'applications, de l'inspection SSL et, cerise sur le gâteau, du contrôle d'accès au réseau sur l'équipement désirant se connecter dessus. FortiWiFi-60C est une version Wi-Fi dédiée au sans fil.

CARACTÉRISTIQUES

PROCESSEUR FortiASIC fonctionnant sous l'OS FortiOS LOGICIEL DE CONFIGURATION FortiExplorer PORTS 5 gigabits, 2 10/100, 2 WAN, 1 DM2, 2 USB PRIX 419 € HT

> DFL 260, D-Link

Parmi les fonctions de cet UTM, un pare-feu doublé d'un système IPS, accompagné d'un antivirus et d'une fonction de filtrage de contenu web et d'URL avec également des fonctions de routage. Le pare-feu examine dans le flux la présence ou non de virus sans nécessité de stocker. La base employée est celle de Kaspersky. La fonction VPN supporte jusque cent tunnels en parallèle et supporte les protocoles IPSec, PPTP et L2TP. Interface web ou ligne de commande ou encore connexion SSH pour gérer l'ensemble.

CARACTÉRISTIQUES

PORTS 4 ethernet 10/100Base-TX, un port 10/100Base-TX Wan et un port DMZ configurable, un port console de type RS 232 PRIX 629 € HT

> XTM 2 Series, Watchguard

Composée de trois éléments, cette série propose des fonctions de pare-feu incluant l'inspection dynamique, l'inspection au niveau de la couche applicative et des proxys applicatifs. Contre les menaces, vous disposez d'un antispyware, d'un filtre contre les attaques DDoS, ainsi que de la surveillance des paquets fragmentés ou malformés et des menaces combinées … Une fonction concernant la VoIP est également présente. Puis en s'abonnant, on peut activer les options de sécurité courantes.

CARACTÉRISTIQUES

PORTS 3 cuivre 10/100, 3 10/100/1000, 2 USB NOMBRE DE NŒUDS PRIS EN CHARGE Illimité, de 100 à 200 authentifications locales d'utilisateurs PRIX 440 € HT

Release by TEAM-DZ

RÉGLAGE D'UN UTM À l'installation

> GESTION RAPPORT L'écran d'administration principal affiche les politiques de sécurité appliquées à chaque port, comme dans le cadre de tout firewall classique.

> ASSOCIATIONS Chaque politique est appliquée aux groupes d'utilisateurs… ce que ne permettent généralement pas les firewalls logiciels pour poste de travail. Cette granularité peut être associée à des règles de contrôle d'applications.

> PRÉCISIONS C'est dans la finesse des paramètres de filtrage et des exceptions que se forgent les niveaux de défense. Un détail souvent utile lorsque certaines alertes d'éditeurs préconisent le blocage temporaire d'extensions précises.

> COMPROMIS La meilleure et la pire des choses : le traçage des opérations courantes et l'enregistrement/avertissement des exceptions. Trop de « log » noie l'information, pas assez enlève tout espoir de « preuves » en cas d'intrusion.

logiciel Security Essential) pour les utilisateurs de « small business server » de moins de dix postes.

Une grande variété de services

Voilà pour le modèle économique de l'UTM. Techniquement, cet hybride est bien plus complexe à saisir. Car comme tous les hybrides, il ne possède aucun gène stable. Certains UTM se limitent à un couple firewall/antivirus/antispam, d'autres intègrent la gestion des canaux de communications chiffrées, d'autres encore des passerelles Voix sur IP, de plus en plus on rencontre des UTM/routeurs (ainsi les derniers modèles de D-Link). La mode est aux WAF (firewall de protection contre les attaques visant les application web) ? En voilà sur les UTM. En d'autres termes, l'UTM, c'est un peu comme les « bouquets télévision » : dès qu'un thème est à la mode, il est susceptible d'entrer dans l'offre à un prix d'autant moins élevé que le nombre d'options choisies dans le bouquet est élevé. D'ailleurs, beaucoup de vendeurs d'UTM commercialisent leurs offres multiservices sous la forme d'un catalogue d'options : matériel et facture à géométrie variable, donnant à l'usager l'impression qu'il maîtrise ses coûts d'un bout à l'autre de la chaîne. Aussi scrupuleux soit-il, un éditeur-intégrateur d'UTM doit lui aussi opérer des choix. Celui des composants qu'il envisagera d'intégrer dans ses boîtiers, des partenaires avec qui il signera des contrats OEM. Car tous les éléments d'un UTM ne sont pas « faits maison », certains éditeurs, tels F-Secure, Check Point, Sourcefire, sont spécialisés dans la vente de licences OEM de leurs produits à destination des fabricants de boîtier « tout en un ». La macédoine qui résulte de ce savant mélange est souvent heureuse, mais jamais parfaite. Ces choix feront que tel UTM, réputé pour la qualité de son firewall, se montrera moins puissant en matière de lutte antivirale. Ou l'inverse. Une situation qui contraint le client à accepter les compromis dictés par l'intégrateur en particulier sur les clauses de support en ligne. Mais à ce prix-là, peut-on le leur reprocher ? ■

UTM : PAS SEULEMENT POUR LES TPE

L'immense majorité des UTM est utilisée par des petites structures dépourvues de véritable service informatique. Ce « prêt-à-porter » de la sécurité tente toutefois d'attaquer deux marchés d'envergure : celui de la sécurité managée par des opérateurs télécoms (des UTM livrés en « bundle » avec un abonnement d'accès à internet) et administrés par ceux-ci et le secteur des grandes entreprises à petites succursales ou franchises régionales.

EXPERTISE

Infections contournant les systèmes de protection

> GUILLAUME LOVET, SPÉCIALISTE SÉCURITÉ, FORTINET. ***« Les technologies de sécurité visant à empêcher ou limiter de façon générique l'exploitation des failles logicielles dans les systèmes d'exploitation modernes (ASLR, DEP…) sont de plus en plus répandues. Désormais, la plupart des systèmes en font usage, par défaut. Les logiciels ne sont pas en reste, Google Chrome et Adobe Reader usant maintenant du Sandboxing. Cette évolution complique sensiblement le travail des cybercriminels, qui, ces dernières années, avaient fait de la faille logicielle la principale voie d'entrée dans le système de leurs victimes. En 2010, nous avions déjà noté que des rootkits, comme Alureon, parvenaient à contourner certains systèmes de protection avancés dans Windows 7 (exécution de drivers non signés), notamment en corrompant l'étape de lancement du système. Il est donc possible qu'en 2011, les cybercriminels implémentent quasi-systématiquement des moyens pour contourner ces systèmes, par exemple en utilisant des techniques qui émergèrent en 2010, du type JIT Spraying… Ou en inventant de nouvelles. »***

Release by TEAM-DZ

L'IDS-IPS : un chien de garde à dresser

Lorsque les outils « à signature » (antivirus, antirootkits, antispam, firewall) ne peuvent plus rien, **les systèmes d'analyse du trafic et de l'activité serveur** entrent en scène pour réagir aux situations anormales.

À SAVOIR

Les IDS/IPS constituent le « haut de gamme » des solutions de protection pour agences et TPE, car exigeant un minimum de temps consacré à l'administration et un budget gravitant entre 2000 et 10 000 euros selon configuration

Au début du monde informatique, rares étaient les programmes de protection… rares étaient les pirates. Rares mais pas inexistants. Le premier à imaginer les fonctions d'un système de détection d'intrusion fut Fred Cohen (All.net), également inventeur des « deception tools », les tout premiers « réseau leurre » ou honeypot.
L'idée de Fred Cohen était d'enregistrer, par un examen du trafic réseau, tout usage anormalement élevé d'une ressource particulière (disque, accès à une base de données) pour en tirer un signal d'alarme. On était alors au milieu des années quatre-vingt. Peu à peu, le principe a évolué et a consisté à associer à chaque profil utilisateur, un outil d'analyse statistique, dont le résultat serait capable de mieux mettre en évidence une activité totalement inhabituelle… donc très probablement irrégulière. Si Monsieur Boulier, comptable, doit régulièrement consulter les données économiques de l'entreprise, ce même genre de consultation par Monsieur Trachon, chef de production à l'atelier d'assemblage provoquera une alerte et un examen suivi de chaque opération informatique dans un journal d'événements. Charge à l'administrateur réseau de prendre la décision qui s'impose, en fermant la porte du réseau au nez de l'intrus ou en validant l'activité. Les IDS étaient nés, et avec eux les prémices de ce que l'on appellera l'analyse comportementale.

Ne confondez pas IDS et firewall

Il est important à ce stade de bien distinguer le rôle de l'IDS de celui du coupe-feu ou firewall. Le premier surveille l'activité du réseau ou d'un serveur, le second « filtre » les entrées et les sorties dudit réseau vers le monde extérieur (ou vers un autre segment réseau, extranet, etc.). Ce sont des outils complémentaires et non pas concurrents.
Très rapidement, les géniaux inventeurs des IDS se sont rendus compte que la surveillance de l'activité réseau ne suffisait pas à déceler l'activité d'un intrus. Si monsieur Boulier (ou un « blackhat » se faisant passer pour lui) échange des requêtes SQL avec le serveur de base de données comptable de l'entreprise, l'IDS trouvera cela légitime. En revanche, un agent situé sur ledit serveur, ayant enregistré le profil statistique de requêtes légitimes de Monsieur Boulier sonnera l'alarme si celui-ci demande la liste des bulletins de salaire de tous les employés sur dix ans. Cette nouvelle génération d'outils de détection d'intrusion installée sur les serveurs s'appelle HIDS, pour « Host Intrusion Detection System », outil de détection d'intrusion dédié serveur. Les « vieux » IDS réseau ont été rebaptisé NIDS (Network IDS) pour éviter toute confusion. Si ces chiens de garde automatiques sont conceptuellement efficaces, ils n'en sont pas moins faillibles. Et ce pour plusieurs raisons.

Tout est une question de seuils d'alerte

En premier lieu, un bon chien de garde doit être dressé à n'aboyer que lorsqu'il flaire un véritable opposant méchant. Il lui faut pour ce faire subir une phase d'apprentissage durant laquelle il constituera ses règles comportementales. Avant cette période, il aboiera sans relâche, et seul un administrateur humain sera capable de lui expliquer « tais-toi, Médor, c'est Monsieur Boulier ». Mais même le comptable peut parfois avoir besoin de sortir de sa routine. Médor-IDS/HIPS risque

3 questions à … | Yann Le Borgne

Windows News: Quelle utilité pour un outil IDS-IPS en PME?
Yann Le Borgne : Aujourd'hui, les PME ont le même degré d'exposition à internet que les grandes sociétés et ne sont pas forcément équipées. Les attaques modernes utilisent comme point d'entrée les mails de phishing ou l'hameçonnage via les réseaux sociaux. Toutes les sociétés, petites, moyennes ou grandes, sont égales devant ce risque .
WN: Pour quelle taille d'entreprise doit-on commencer à se poser la question de la présence d'un tel outil?
YLB : La taille importe peu. Le facteur déclenchant d'un tel besoin est plus lié à deux thèmes principaux: le secret industriel (R&D, Brevets, dossiers clients sensibles avec besoin de confidentialité extrême) et lla spécificité de l'application sur internet (l'activité est-elle réalisée via ou grâce à internet?)
WN: Pour une PME qui n'a pas les moyens techniques et financiers de posséder des compétences internes en sécurité, doit-on envisager l'IPS dans le Cloud? Ce type de services existe-t-il?
YLB : Les services managés (MSS) tendent à se démocratiser rapidement. En France, certaines collectivités locales, par exemple, équipées d'IPS délèguent leur gestion à une société de services.

« Toutes les sociétés, petites, moyennes ou grandes sont égales devant les risques informatiques. »

Yann Le Borgne
Expert Sécurité chez Sourcefire

Release by TEAM-DZ

donc d'aboyer pour un oui ou pour un non (on appelle ce genre d'alerte un « faux positif »), ou se taire si les règles de dressage ont été levées de manière plus permissive (faux négatif, cas le plus problématique). Cette situation devient rapidement intenable, car l'usage d'un IDS entraîne très rapidement l'administrateur à passer quelques nuits blanches derrière le cahier des événements afin de vérifier la validité des alertes. Au début des années 2000, quelques équipementiers décident donc de dresser Médor à ne plus aboyer, mais à courir au devant de l'intrus et lui bloquer le chemin en montrant les dents. Ce sont les premier IPS, ou Intrusion Prevention Systems. Une anomalie dans le trafic (attaque par fragmentation par exemple, requête SQL massive, tentative d'écriture imprévue sur une ressource…) va déclencher une action correspondante: blocage de la session de requête SQL, rejet ou blocage de la trame, intervention d'un mécanisme antivirus associé… L'administrateur n'intervient qu'au moment de la phase d'apprentissage. Phase d'autant plus courte que, depuis le temps, les équipementiers ont eux aussi affiné les algorithmes et règles d'analyse comportementales. Un IPS est, à notre époque, généralement vendu avec un certain nombre de règles comportementales génériques prédéfinies. Quel sera le stade suivant? Très probablement la disparition physique des IDS/IPS. L'expertise nécessaire au déploiement de ces équipements est souvent sous-traitée auprès de sociétés de service externes, qui « prennent la main » à distance. Ce sont les « services managés ». ■

Les obligations légales des PME

> OLIVIER ITEANU, AVOCAT À LA COUR.

« Il n'existe pas à ce jour d'obligations légales à la charge des entreprises pour protéger leur système d'information. La jurisprudence tend à rendre ces entreprises responsables quand elles ne prennent pas certaines mesures. Elles peuvent donc être victimes d'une attaque et… responsables juridiquement. Ainsi, la loi informatique et libertés punit toute entreprise qui n'a pas pris des « précautions utiles » pour préserver la sécurité des données à caractère personnel, de cinq ans de prison et 300000 euros d'amende. Dans l'affaire Tati contre Kitetoa, la Cour d'Appel de Paris a relaxé, en 2002, un journaliste entré dans une partie non autorisée du site Tati, car il l'avait fait par une faille signalée mais non réparée.

Achat | Trois filtres pour PME

> Intrushield i-1200, McAfee

Chez McAfee, le plus petit des IPS/IDS dédié s'appelle Intrushield I-1200. Spécifiquement destiné aux TPE, succursales et agences, il accepte 40 000 connexions simultanées et n'intègre que quatre ports Fast Ethernet 100 Mb/s (un port de gestion, trois de réponse). Il a été conçu pour être installé dans un rack et se montre particulièrement efficace pour les attaques par déni de service (DDoS). Il fait partie d'une gamme étendue d'IPS/IDS.

CARACTÉRISTIQUES

DÉBIT FILTRÉ 100 Mb/s sur deux ports, partagés jusqu'à 16 IDS virtuels PROTECTION Par firewall, stateful failover PRIX 6,8 kg PRIX 2232 € HT

> FAST360, Arkoon

Ce constructeur Français propose un modèle d'entrée de gamme intégrant trois ports gigabit dont un switch quatre ports. Comme cet équipement entre également dans la catégorie des UTM, cet IPS/IDS a l'avantage d'intégrer les firewalls et autres « antitout » sur lesquels l'IDS peut directement envoyer ses ordre de « coupure » en cas d'alerte. Ils ont été étudiés pour être mis à jour en temps réel, vingt-quatre heure sur vingt-quatre et à distance. Le Fast 360 supporte pour le filtrage applicatif plus de 20 protocoles.

CARACTÉRISTIQUES

DÉBIT FILTRÉ 40 Mb/s sur 4 ports Gigabit, 10 utilisateurs (existe en modèle Small 90 utilisateurs illimités), certifié EAL2+ PRIX À partir de 938 €

> 3D500, Sourcefire

C'est probablement là le premier détecteur d'intrusion « historique », qui a vu le jour sous forme d'IDS totalement logiciel Open Source, soutenu par une très importante communauté de développeurs qui se sont attachés à enrichir la base de règles. Sous sa forme commerciale, cet IDS/IPS s'adresse aussi bien à de petites structures (avec notamment le modèle 3D500 offrant 5 Mb/s de vitesse de ligne) qu'à des réseaux de grande taille exigeant des débits jusqu'à 10 Gb/s.

CARACTÉRISTIQUES

DÉBIT FILTRÉ 5 Mb/s sur 4 ports Gigabit FILTRE SPÉCIFIQUE Pour Oracle, Firefox, Gnutella, Timbuktu MOTEUR DE DÉTECTION Snort PRIX 2039 € HT

Release by TEAM-DZ

LA SÉCURITÉ DES PC NOMADES

Si les ordinateurs de bureau **doivent craindre les attaques purement informatiques, les outils de mobilité sont exposés à d'autres dangers :** vol de matériels, de données, de minutes de communication. Une approche différente de la sécurité périmétrique.

SOMMAIRE

ATTENTION À LA PRISE USB…
Il est possible d'« injecter » via la prise USB un programme d'espionnage.

MÉFIEZ-VOUS DES MOIS PAIRS
Microsoft ne corrige les trous Internet Explorer que tous les deux mois.

Du virus Android insaisissable à l'agent d'entretien diabolique, en passant par le hacker de réseaux Wi-Fi ou le BlueSnarfer de liens Bluetooth, les menaces informatiques qui touchent le monde de la mobilité s'avèrent aussi innombrables que sont importantes les manchettes des journaux en faisant état. Le spectre d'un virus capable de frapper à la fois les clients Bouygues, Orange et SFR a un je-ne-sais-quoi d'apocalyptique… Mais si les infections menacent une partie de la « mobilité traditionnelle », celle des PC portables, elles semblent se désintéresser des smartphones et de leurs ancêtres : les agendas de poche. Les premières causes de sinistralité des équipements mobiles sont d'une tout autre nature : panne (très souvent des unités de stockage), bris, perte, vol à l'arraché, et utilisation abusive des communications par une personne non autorisée. Le danger de l'informatique mobile, du PC ultraportable au téléphone, c'est précisément sa mobilité et les risques accidentels qui y sont liés. Contre eux, il n'existe pas beaucoup de parades : une bonne assurance vol-accident et une sauvegarde régulière des données. On ne trouve pas d'antivirus capable de contrer les lois de la gravitation, pas de firewall qui protège des chocs, pas d'antispyware qui prévienne de l'approche d'un individu louche. Corollaire de cette logique, si un super-espion industriel ou un techno-truand souhaite faire main basse sur un carnet d'adresses ou la liste précise des rendez-vous d'un cadre supérieur, cela lui coûtera moins cher d'engager un pickpocket que de passer six mois à développer un mégavirus à extraction de données et propagation virale 3G/Bluetooth/SMS/Wi-Fi. C'est principalement pour cette raison que les responsables de flottes de mobiles font peu de cas des antivirus. Certes, côté ordinateurs portables, l'on se doit de posséder, comme toute autre machine, des outils de protection périmétrique classique : firewall, antivirus, antispyware, antirootkit… panoplie à laquelle on ajoutera, sur ses « laptop » comme sur ses téléphones intelligents, un utilitaire de chiffrement qui évitera toute fuite de données en cas de vol. À ceci peut s'ajouter un service

Release by TEAM-DZ

Portables : Wi-Fi, le maillon faible

> LES ESPACES À RISQUE Un ordinateur portable se trouve rarement connecté au monde extérieur par un câble ethernet. C'est le Wi-Fi, avec ses vieux protocoles de protection facilement attaquables, qui est son principal canal d'échange. Ce que l'on sait moins, c'est qu'il existe d'autres programmes de « tests d'intrusion » (Canvas par exemple) capables de compromettre les protocoles les plus récents. Mais ces attaques visent la plupart du temps les bornes d'accès fixes. Les liaisons Wi-Fi les plus vulnérables restent celles des utilisateurs de PC portables se connectant sur une borne publique. La plupart de ces bornes ne sécurisent pas (ou très mal) la liaison entre l'ordinateur et le point d'accès, notamment au moment de la toute première connexion.

capable d'effacer à distance les informations contenues dans l'espace de stockage de l'appareil et un programme capable de suivre à la trace un terminal ou un ordinateur à chacune de ses apparitions sur le réseau téléphonique ou internet. Parfois même, ces programmes de sécurité intègrent une commande « suicide » qui peut soit se déclencher en cas de non-connexion prolongée au réseau d'entreprise, soit s'activer à partir d'une console d'administration centrale. De prime abord, tout cela paraît simple.

> ON N'A PAS D'ANTIVIRUS CAPABLE DE CONTRER LES LOIS DE LA GRAVITATION, **PAS DE FIREWALL QUI PROTÈGE DES CHOCS,** PAS D'ANTISPYWARE QUI PRÉVIENNE DE L'APPROCHE D'UN INDIVIDU…

Une protection par type d'appareil

Si, pour l'heure, aucune apocalypse virale, aucune grande razzia numérique n'a frappé un réseau de téléphones, c'est grâce à la multiplicité des systèmes d'exploitation et à la proportion encore faible des téléphones dits « intelligents ». Cette hétérogénéité rend assez complexe et peu efficace l'écriture d'un code d'attaque généraliste. Les constructeurs et équipementiers préfèrent proposer, avec tout contrat lié à une flotte de mobiles, des logiciels de gestion des comptes et de protection des appareils. Ainsi RIM, avec son serveur BES Express pour petites et moyennes structures, destiné à sécuriser les accès au réseau d'entreprise. Techniquement, il est toujours un peu plus aisé de construire un outil de protection pour 4 types de plateforme que d'écrire un virus universel. Certains éditeurs parviennent même à développer un outil compatible avec les 4 ou 5 systèmes d'exploitation de mobiles les plus courants, le tout gérable à partir d'une console d'administration unique. C'est le cas de Mobiquant, entreprise française qui prend en compte les Blackberry, iPhone, appareils sous Windows Mobile, Android, Bada, Windows 7 ou Symbian. L'on pourrait citer également Good Technology (Iphone/IOS, Android), LANDesk Handheld Manager (Palm, Windows Mobile, Symbian…), DeviceLock pour mobiles (plus apparenté à de la gestion d'accès) ou F-Secure Anti-Theft for Mobile qui « télé-assassine » les données à distance, par simple envoi d'un SMS.

Faites preuve de bon sens avant tout…

Reste que 90 % des « mobiles » en service sont utilisés tant par des particuliers que par des TPE, petites PME, professions libérales, pour qui l'installation d'un serveur d'administration ne se justifie par pour surveiller 2 à 10 téléphones et autant d'ordinateurs portables. Ces

Release by TEAM-DZ

usagers doivent alors « faire à la main » ce que les logiciels de sécurité intègrent automatiquement. À commencer par la gestion d'un mot code d'accès (PIN) qui ne soit pas le « 0000 » d'origine. En activant ou en installant également les fonctions de chiffrement disponibles sur chaque plateforme… sans pour autant apporter une confiance absolue dans ces mécanismes. Car si les algorithmes de chiffrement demeurent généralement très solides, la manière dont ils sont intégrés à un système d'exploitation mobile laisse parfois à désirer. L'ancêtre de Windows Mobile avait son mot de passe protégé avec un outil ridiculement simple (une opération EXOR sur le mot Pegasus écrit à l'envers). Pas plus tard que l'an passé, le chiffrement de l'iPhone 3GS a succombé sous les coups d'un hack relativement simple. Outre le chiffrement et ce, qu'il s'agisse d'un téléphone ou d'un ordinateur portable, la première des prudences consiste à « décommissionner » l'appareil à chaque retour de mission, autrement dit d'en purger les espaces de stockage de toute donnée importante qui ne sera pas indispensable lors des futurs déplacements. Cette règle « d'hygiène numérique » reste hélas peu observée, et il n'est pas rare de trouver sur ces « post-it » modernes que sont les iPhones, Android et Windows Mobile, des notes !

À SAVOIR

Le plus surveillé et le plus volé

L'iPhone 4 : à partir de 630 euros, assurance antivol… non comprise !

Les points faibles des mobiles

Ils sont quasiment innombrables, et on en découvre de nouveaux chaque jour. Les attaques Wi-Fi, bien sûr, ainsi que les intrusions via un port Bluetooth font souvent l'objet d'articles alarmistes dans la presse. Les ports USB et eSata également, qui peuvent servir à démarrer une machine à partir d'un disque externe ; celui-ci donnera ensuite accès aux ressources internes de l'ordinateur portable. L'on oublie en revanche un peu trop souvent le port Firewire/IEEE-1394, qui, avec quelques logiciels spécialisés, autorise l'accès tant aux données en mémoire vive (memory attack) d'une machine qu'à ses ressources disque. Les réseaux 3G enfin, peuvent potentiellement servir à conduire des attaques via SMS ou par « drive-by download » (téléchargement d'une appliquette Java, par exemple, en visitant un site web qui semble anodin). Parfois même, certaines intrusions sont rendues possibles grâce à l'utilisateur lui-même, ainsi les possesseurs d'iPhones « jailbreakés » qui oublient de modifier le mot de passe d'administration de leur téléphone (Alpine par défaut). Contre ce genre d'omission, aucun antivirus ne peut protéger quoi que ce soit. ■

Focus | Attention à la prise USB de votre machine

■ Les risques les plus courants sont d'une grande simplicité… Il existe une multitude d'attaques permettant d'« injecter » via la prise USB un programme d'espionnage de type rootkit. L'un des chercheurs les plus connus dans le domaine de la sécurité, Joanna Rutkowska, a démontré comment une « femme de chambre diabolique » pouvait installer, à l'insu du propriétaire d'un ordinateur portable, un logiciel espion capable de s'affranchir même de certains programmes de chiffrement des données… tout çà, en utilisant une simple clé USB et sans avoir à « casser » le mot de passe d'ouverture de session. Et nul besoin de recourir à des opérations relativement techniques, un bon informaticien peut aisément piller le contenu d'un disque dur simplement en démarrant l'ordinateur à partir d'un disque externe branché sur port USB. La contre-attaque ? Chiffrez vos données importantes, voire la totalité de votre disque dur. Ne laissez jamais un PC portable sans surveillance, même et surtout dans une chambre d'hôtel à l'étranger.

Pratique | Protégez-vous des risques

1 ANTIVIRUS NetQin, Lockout, DroidSecurity, etc. les antivirus gratuits pour téléphones mobiles ne sont pas très difficiles à trouver… Mais parfois, l'effet placebo reste aussi efficace qu'un véritable remède !

2 ANTIVOL Le premier risque encouru par un appareil mobile, c'est le vol, et le second, l'extraction de données. La solution ? Surveillance, câble en acier et outil de chiffrement (souvent gratuit).

3 LOGICIEL DE PROTECTION CENTRALISÉ Contre le vol de communications et de données, une gestion des comptes centralisée et une séparation des espaces « travail » et « personnel » s'imposent.

Release by TEAM-DZ

La chasse aux vulnérabilités est ouverte

Un système bien « patché » peut contrer **une attaque virale que pourraient laisser-passer les antivirus et les UTM les plus perfectionnés.** Et quand les premières lignes de défense tombent, l'arrière doit se montrer « solide ». C'est là que réside toute la science de la gestion des correctifs logiciels.

L'invasion du virus Conficker en est la preuve éclatante : ce ver exploitait un défaut de Windows corrigé depuis, mais que de nombreuses grandes entreprises n'avaient pas pris soin de répercuter sur leurs postes. Comble de malchance, sa propagation est passée inaperçue à la quasi-totalité des antivirus les plus connus. Pourtant, face à un ordinateur régulièrement mis à jour, même dépourvu d'antivirus, celui-ci n'avait aucune chance. Mais Conficker et sa faille Windows ne sont qu'un exemple parmi tant d'autres. Les récentes attaques contre Google Chine, Adobe ou certains grands groupes industriels américains n'ont été possible que grâce à des trous de sécurité, généralement situés dans des logiciels « non Microsoft ». Au hit-parade des défauts de fabrication : Java de Sun/Oracle, l'ensemble des outils utilisant le format de fichiers pdf, Flash Player, parfois même Firefox… bref, tous les programmes les plus populaires qu'un pirate s'attend à trouver sur une machine quelconque. Ce qui permet d'énoncer la première règle d'or du correctif bien tempéré : le « mardi des rustines » de Microsoft ne sera pas ton unique arme anti-faille.

Petite panoplie des outils gratuits et payants

Le bouche-trou le plus utilisé reste le célèbre Windows Update et son pendant pour entreprise, le serveur Windows Server Update Services (alias Wsus), en téléchargement gratuit et actuellement en version 3.0/SP2. Wsus concentre les mises à jour et évite ainsi que tous les postes d'un réseau téléchargent N fois un même bouchon de sécurité. Un détail qui, en l'absence de serveur, risque d'entraîner un écroulement des accès internet le jour de la sortie d'un service Pack. En outre, Wsus s'avère capable de planifier les déploiements de rustines pour ne pas perturber le bon fonctionnement du réseau local. À cet outil doit être adjoint un « vérificateur d'applications » (ou d'inventaire de failles), qui s'assure que chaque rustine a bien été installée. Car certains virus bloquent ou corrompent les mises à jour, lorsque ce n'est pas la faute à un accident de réseau. Longtemps, ce rôle était assuré par HFNetChk, une version « allégée » et gratuite de la plateforme de sécurité Shavlick (www.shavlik.com). Cet éditeur continue d'offrir un outil d'analyse à distance et gratuit pour les particuliers et petites structures. Mais depuis trois ou quatre ans, c'est Secunia, avec son Personal Sofware Inspector, PSI (http://secunia.com/vulnerability_scanning/personal), qui a raflé la place d'outil d'inventaire le plus utilisé dans le monde. La version entreprise de PSI s'appelle Corporate Software Inspector, et tous deux détectent et corrigent les imperfections logicielles de tous types… Windows, mais également Adobe, Sun, Skype, iTunes, les contrôles ActiveX ésotériques. Certains concurrents tels F-Secure ont tenté d'occuper ce même marché, mais avec moins de succès. Le Health Check de l'éditeur danois (www.f-secure.com/en_EMEA-Labs/security-threats/tools/health-check) s'est vite alourdi de fonctions périphériques, telles la sauvegarde de

3 questions à… | Nicolas Ruff

Windows news Qu'existe-t-il pour les PME pour détecter les failles de leur système ?
Nicolas Ruff : Il existe des scans gratuits peu efficaces car ils fonctionnent avec l'adresse IP de celui qui le lance. Il faut privilégier le scan du réseau interne. En effet, la majorité des compromissions arrive maintenant via les e-mails ou par une clé USB infectée par la navigation sur des sites douteux.

WN Y a-t-il des offres sur le marché pour réaliser ces scans ?
NR : Des sociétés comme Qualys fournissent des appliances à installer dans l'entreprise pour les failles du réseau interne, ou différents services de scan (gratuits) dans le cloud, dans le cas de l'examen d'une machine donnée. Si beaucoup de failles sont détectées, il faut ensuite réagir et réaliser des inventaires, gérer des configurations logicielles… et là, cela devient réellement difficile à soutenir pour une PME. Les produits, tels que Secunia, restent plus appropriés car non seulement ils scannent mais ils donnent également une liste des applications vulnérables, tout en installant automatiquement les correctifs nécessaires. La connaissance de ce type d'applications n'est qu'un début, il faut savoir ensuite les maintenir.

WN Quels conseils donner à une PME pour l'aider à gérer ses failles ?
NR : Avec une application comme Secunia, on ne couvre pas loin de 80 % des risques liés à l'informatique aujourd'hui. D'une façon générale, quand il s'agit d'une faille technique, on règle le problème avec des produits.

« la majorité des compromissions arrive via les e-mails ou par une clé USB infectée… »

Nicolas Ruff
Chercheur en sécurité chez EADS.

Release by TEAM-DZ

3 questions à… | Christophe Bianco

Windows news La chasse aux failles est-elle à la portée des TPE-PME?
Christophe Bianco: Cette catégorie de sociétés a aujourd'hui les mêmes préoccupations que les plus grandes d'entre elles, mais sans budget et ressources identiques. Et pourtant, tôt ou tard, du fait de l'interconnexion des systèmes d'information entre client et fournisseur, il sera demandé à l'entreprise de petite taille de justifier du niveau de sécurité de son système. Les diverses réglementations, désormais obligatoires pour chaque secteur professionnel, induisent la démocratisation de la chasse aux failles.

WN Est-ce que la sécurité « cloud » participe à cette démocratisation?
CB: Le cloud permet aux entreprises de travailler sans investissement et de ne payer que pour son utilisation. La sécurité en mode SaaS, Software as a Service, reste plus facile à adopter tout en réduisant les coûts… Ce qui est important pour une PME, c'est le fait d'être opérationnelle et non de se savoir en environnement sécurisé.

WN La prise de conscience des PME s'améliore-t-elle?
CB: Il s'agit plutôt d'une connaissance de proximité que d'une réelle prise de conscience, du fait de l'information générale. La prise de conscience se fait lorsque le client demande à son fournisseur de justifier du niveau de sécurité de son système d'information, ou lorsque l'entreprise essaie d'être conforme aux réglementations, ou encore quand elle se fait attaquer.

« Tôt ou tard, il sera demandé à l'entreprise de petite taille de justifier du niveau de sécurité de son système. »

Christophe Bianco
Vice-président Europe chez Qualys.

photographies, peu en rapport avec l'inventaire de failles. Il est à noter que ces « scanners de failles » utilisent de plus en plus des bases de données distantes et un moteur d'analyse également distant. Ces services « cloud computing » possèdent donc l'énorme avantage d'être toujours « à jour », et l'inconvénient de ne plus pouvoir fonctionner si l'accès à internet est désactivé. Un nombre croissant de virus tente de bloquer tout spécialement les sites de ces services de sécurité. Les habitués des pages web du Technet le savent bien : il existe deux types de messages sécurité chez Microsoft : les alertes et les bulletins. Les bulletins signalent l'existence d'une faille et pointent sur les correctifs colmatant ledit trou de sécurité ; les alertes préviennent du défaut… un point c'est tout. Ces alertes sont émises lorsqu'une faille est utilisée (exploitée) par des personnes mal intentionnées et qu'aucun correctif ne se trouve encore disponible. Dans ce cas précis, le passage le plus important à lire se trouve dans la section « mesures de contournement » de l'alerte en question, lequel explique généralement comment, par le biais de l'outil *Regedit*, l'on peut désactiver la partie « malade » de Windows et ainsi éviter de se faire attaquer. Ces mesures provisoires, parfois handicapantes et compliquées à mettre en œuvre, sont de plus en plus automatisées grâce à des scripts rédigés par les ingénieurs de Microsoft, les fameux « Fixit » du Microsoft Fixit Solution Center (http://support.microsoft.com/fixit). Lorsque le trou de sécurité concerne un logiciel non Microsoft, il s'avère souvent difficile d'obtenir une information claire de la part des différents éditeurs. Quand, pourquoi, comment supprimer ou désactiver provisoirement un Flash Player? Une fonction spéciale du navigateur Firefox? C'est le rôle rempli par certains sites officiels d'informations, à commencer par le Cert dédié à l'industrie française (www.cert-ist.com), le SANS Internet Storm Center américain (http://isc.sans.edu/diary.html), le Cert US (www.us-cert.gov/cas/techalerts), le Mitre, également américain, et qui tient à jour la totalité des failles répertoriées Windows, Linux, OS X et autres (http://cve.mitre.org). Terminons cette liste par le remarquable travail d'un ancien journaliste du *Washington Post*, Brian Krebs, qui prévient, avec une régularité métronomique et sans jargon technique imbuvable, des moindres dangers relatifs aux failles de sécurité (http://krebsonsecurity.com).

Un monde de légendes…

En termes de vulnérabilités, les vendeurs et partisans d'un clan ou d'un autre font souvent assauts de mensonges et de contre-vérités. Petit florilège des idées reçues : il y a moins de bugs dans les environnements Apple que dans l'univers Windows. Faux. En nombre moyen de failles officiellement découvertes, les résultats restent pratiquement semblables.

Des sources d'information qui se tarissent

> OBSERVATEURS D'ÉVÉNEMENTS Si le Cert, le SANS, le Mitre signalent l'existence de la moindre faille « officiellement répertoriée », l'on constate un très net recul du côté des sites techniques plus exhaustifs. Milw0rm, qui répertoriait tous les programmes d'exploitation dangereux, a fermé ses portes depuis bientôt un an. Les listes de messagerie (ML) autrefois techniques ne sont plus informatives comme par le passé. Les chercheurs de vulnérabilité ont tendance à moins « publier » leurs découvertes, surtout depuis qu'ils parviennent à vendre le fruit de leurs recherches aux entreprises spécialisées, telles le Zero Day Initiative (ZDI, www.zerodayinitiative.com), ou espèrent empocher la « 3L33t Prime » de Google (3133,70 $). Parallèlement à cette tendance, on constate un regain d'intérêt des services de l'État pour des trous « exploitables à distance » échappant aux outils d'inventaire de failles… Au niveau international, les failles « confidentielles » demeurées secrètes sont utilisées dans des opérations de cyber-espionnage à grande échelle (les fameuses « APT » ou Advanced Persistent Threat).

Release by TEAM-DZ

JARGON

Faille ou trou logiciel. Défaut interne à un logiciel (système ou application) susceptible de pouvoir provoquer une action mettant en péril un ordinateur : déni de service, accès distant, vol d'informations, élévation de privilèges, exécution de programmes… ou plantage pur et simple.

Exploit Méthode capable de tirer parti d'une faille. Certains exploits ne peuvent offrir que des privilèges limités (sur la console locale) ou peu utiles. D'autres ouvrent à distance une porte sur le cœur du système compromis (en argo : « sploit »).

Pownеd (expression argotique). Machine ou application compromise.

Rustine, patch, correctif Verrue logiciel venant généralement masquer un trou de sécurité (sans le supprimer toutefois).

Mesure de contournement Action visant à éliminer un risque d'attaque par exploitation d'une faille, en bloquant l'accès à la partie « malade » du code. Généralement, une mesure de contournement se contente de désactiver le mécanisme à risque, ce qui parfois peut avoir des conséquences dans l'utilisation quotidienne d'un ordinateur (blocage d'ActiveX par exemple).

Il demeure en revanche exact que les vecteurs d'attaque (virus, exploits divers) sont statistiquement moins nombreux sur Mac que sur PC… simple question de taille de cible et de « rentabilité ». Même les auteurs de virus calculent leur retour sur investissement. Cette même remarque s'applique également aux systèmes Linux. Une équipe de développement commet autant d'erreur qu'une autre. Cela reste un problème humain, et non une question de noyau. Le système Windows est le logiciel qui compte le plus de failles exploitables : c'était vrai… autrefois ! Depuis la génération Vista, d'importants efforts de nettoyage de code ont été prodigués par Microsoft. Désormais, il se développe plus de virus tirant parti de failles Java ou Adobe que d'infections purement Microsoft. À souligner que les défauts Java et Adobe sont généralement exploitables de manière semblable (mais avec des conséquences différentes), tant sous Windows que sous OS X ou Linux. La publication d'un correctif ferme la porte à certains virus : pas toujours exact. C'est parfois même le contraire. En analysant la manière dont un éditeur comble une faille, un développeur d'exploits peut « retrouver » par processus d'ingénierie inverse la faille originelle et cibler ainsi les machines qui n'ont pas été rapidement corrigées. Quelques virus continuent de vivre plus de cinq ans après la diffusion d'une rustine. Certains correctifs provoquent des blocages, il faut parfois refuser de les appliquer : exact. Ces situations exceptionnelles justifient les périodes de « test de régression » en usage dans certaines grandes entreprises, tant en France qu'à l'étranger. Celles-ci possèdent d'autres moyens de protection leur permettant souvent de supporter le risque provoqué par ce sursis. Dans le cadre d'une plus petite structure, le déploiement doit primer sur le risque du blocage car il est mathématiquement inférieur au risque d'exploitation ou d'infection. Un système d'exploitation installé dans une machine virtuelle ne risque rien : faux. Même dans une « VM », un système reste relié à un réseau, parfois à internet, et son niveau de protection demeure fonction de la solidité des défenses périmétriques locales et réseau. Autrement dit, strictement identiques à celles d'une machine physique normale.

Attaque : critique ou importante ?

Un appareil isolé de toute connexion internet ne risque rien : faux. Sans accès au web, pas de mise à jour possible, tant des antivirus que des installations de correctifs (à moins que ledit réseau dispose d'un serveur-passerelle chargé de la fourniture des correctifs). Sans ces mises à niveau, n'importe quelle attaque via un périphérique de stockage mobile (clé USB, disque dur externe…) aura toutes les chances de s'installer avec succès. Une faille « importante » est moins dangereuse qu'une faille « critique » : ni vrai, ni faux… personne ne peut savoir. La notion de criticité d'une faille varie d'un éditeur à l'autre et d'un organisme à l'autre. Pour certains, « critique » veut dire « il existe un exploit tirant parti de cette faille ». Ce qui est à distinguer de : « il existe un virus trouvé dans la nature tirant parti de cette faille ». Parfois, l'existence d'un exploit se limite à un module de logiciel de test de pénétration. Critique qualifie également les trous de sécurité même sans exploit mais dont on peut estimer qu'ils peuvent être utilisés à distance. « Important » reste souvent attribué aux attaques simples, telles qu'un déni de service ou une exploitation « locale » (présence physique sur l'ordinateur visé). Un déni de service sur un serveur web marchand, c'est « important » ou « critique » pour son propriétaire ? Une élévation de privilège sur une base de données via un accès console, c'est « important » ou « critique » pour un administrateur ? Tout demeure question de circonstance. Ceci étant défini, ce distinguo dans les qualificatifs s'accompagne (comme c'est le cas chez Microsoft) d'un « index d'exploitabilité » et donne une idée même imparfaite du degré d'urgence dans la course au déploiement de rustines. **Marc Olanié et Solange Belkhayat**

Méfiez-vous des mois pairs !

> DES CORRECTIFS AU COMPTE-GOUTTES Pourquoi la faille Microsoft dite « MHTML » n'a pas été corrigée en mars dernier, alors qu'elle avait été découverte début février ? Parce que mars est un mois impair et que, exception faite de trous dangereux et activement exploités nécessitant l'émission d'une rustine « hors calendrier », Microsoft ne corrige les trous Internet Explorer que tous les deux mois ! Un laps de temps rendu nécessaire pour assurer une parfaite compatibilité avec l'existant. D'autant plus que les bouchons de sécurité IE colmatent généralement entre 5 et 10 défauts différents d'un seul coup. Le calendrier des correctifs Internet Explorer suit donc une procédure de « tests de régression » stricte de plus de deux mois pour éliminer tout risque de fourniture de « rustine trouée ». Prochains rendez-vous IE en avril, juin et août prochain…

Release by TEAM-DZ

COMPARATIF ■ OUTILS DE CONTRÔLE À DISTANCE

VEILLEZ SUR VOS STATIONS DE TRAVAIL

Les outils de prise **de contrôle à distance rencontrent un vif succès.** De l'assistance technique au travail collaboratif, ces « PC télécommandés » connaissent peu de limites.

LogMeIn
La simplicité et l'universalité pour objectif.

UltraVNC
La solution de référence issue du monde open source.

TeamViewer 6
Le couteau suisse de la prise de commande à distance.

Bureau à distance
L'outil RDP de Windows par excellence.

La mode des ordinateurs portables et des téléphones intelligents a parsemé notre quotidien d'informatique et de connexions réseau. Le courriel tombe sur nos iPhones et Android, les « Netop », ultra-portables, Tablet PC et « Pads » de toutes provenances font de notre vie une succession de sessions et de connexions. Mais ces services de mobilité ont leurs limites, et l'on ne peut imaginer transporter l'intégralité de sa bibliothèque de fichiers sur ces outils portables. Le document stratégique « oublié à la maison », une grève des transports qui interdit toute présence sur le lieu de travail alors que monsieur De Mesmaeker doit précisément signer des contrats de la plus haute importance, un conseil à un ami primo informatisé à propos d'un logiciel de création graphique ou de CAO, qui jamais ne pourra être installé sur un ordinateur portable… autant de cas qui ne peuvent être résolus que par un logiciel d'accès à distance. Un programme qui, généralement, redirige le clavier et l'écran de la station distante que l'on souhaite piloter… mais qui également peut faire bien plus, comme intégrer un programme de transfert de fichiers optimisés reliant la machine hôte et son poste client, ou autoriser l'usager de la machine distante à interagir avec son PC ; une fonction indispensable dans le cadre d'une session de formation ou de démonstration technique.

LES CRITÈRES DE CHOIX

LE CHIFFREMENT Que ce soit sur réseau local ou via le réseau public, tout outil capable d'agir au niveau des fonctions administratives d'un serveur doit impérativement être surprotégé et ses communications chiffrées. Ce n'est pas le cas par défaut de certains logiciels « open », tel VNC.

LES FONCTIONS DISPONIBLES L'outil universel n'existe pas. Entre celui qui possède un utilitaire d'accès à la base de registre, un autre offrant le support de VoIP et un troisième pouvant être supervisé (ainsi le Bureau à distance) par les politiques de sécurité locales, il y a un monde…

LA TRANSPARENCE VIS-À-VIS DU FIREWALL Les outils de prise de contrôle ne doivent pas être bloqués par les protections périmétriques (firewall). Pourtant, bien des routeurs d'entrée de gamme sont incapables de « laisser passer » un canal chiffré de type VPN SSL, ou mieux encore SSL-TLS.

L'activation du service RDP sur l'appareil distant

Premier et principal outil de l'attirail communiquant de Microsoft, la console « bureau à distance » est plus complexe qu'il n'y paraît. Son installation se limite généralement à activer le service RDP sur la machine distante, les services web si l'on souhaite exploiter cette fonction via un navigateur, et à configurer le programme client « connexion bureau à distance ». Il n'en faut pas plus pour prendre la main sur l'hôte, avec les droits liés au couple « login-mot de passe » fournis lors du paramétrage des comptes locaux du PC distant. Le niveau de chiffrement du lien reliant le terminal et la machine distante peut être renforcé par l'installation d'un tuyau SSL-TLS, si la liaison transite par internet, d'autant plus aisément que les services de bureau à distance peuvent aussi être encapsulés dans une couche http. C'est le « Remote Desktop Web Access », anciennement connu sous le nom de « Terminal Services Web Access » (TS Web). Son avantage indéniable demeure de pouvoir distribuer tous les services RDP, habituellement offerts par le client « bureau à distance », mais sous la forme d'une page web. Les temps de réaction sont légèrement plus lents qu'avec le mode natif réservé au réseau local et aux accès distants directs (dits accès « RAS » ou accès sur liaison VPN), mais ne nécessitent pas de logiciel client spécifique. Reste que ce luxe repose, côté machine hôte, sur les

Release by TEAM-DZ

services IIS (Internet Information Server), gros consommateurs de ressources. Machines musclées recommandées. Peut-on tout faire avec le bureau à distance? Non, hélas! Mais l'outil est assez pratique pour administrer un Home Server, transférer des couper-coller de fichiers en série entre les deux ordinateurs ainsi reliés, voire même écouter de la musique ou utiliser un client de téléphonie VoIP distant. Mais point de mode d'assistance « par défaut ». Il en existe pourtant un intégré à Windows, qui utilise les mêmes bases d'outils, mais demande de passer par la procédure de « demande d'assistance à distance », lourde et peu ergonomique. Pas non plus d'échanges vocaux ou vidéo entre correspondants, ou d'affichage commun d'une même session. Dans sa version pour « poste client » Windows (XP, Vista, 7), le client Bureau à distance n'autorise qu'une seule session et déconnecte la personne travaillant sur la machine hôte. C'est en revanche un protocole excessivement rapide et optimisé pour tous ceux qui souhaite télétravailler sur un ordinateur éloigné, et un logiciel qui ne demande pratiquement aucune connaissance particulière. Revers de la médaille, sa simplicité fait parfois oublier certains prérequis important. Un mot de passe faible (ou pire, pas de mot de passe du tout) peut, si l'ordinateur hôte est accessible depuis internet, servir de repaire à tous les pirates, virus et autres infections que le net peut abriter.

TeamViewer: des options à la tonne

TeamViewer, édité par la société allemande TeamViewer, est diffusé sous une multitude de versions: les unes professionnelles, les autres grand public… ces dernières étant gratuites. Ce procédé de marketing viral connaît un succès tel que l'on compte près de 60 millions d'utilisateurs. Les avantages de TeamViewer? Ceux d'un outil multiplateforme (Windows, OS X, Linux, Android, iPad/iPhone, etc.), utilisant un navigateur web pour afficher ses sessions, et assurant trois fonctions principales: accès à distance, assistance et démonstration. L'assistance, par rapport au mode « accès à

> LOGMEIN ■ GRATUIT

Assistant salvateur ou administrateur?

Ce programme se faufile partout, et franchit avec une facilité déconcertante la grande majorité des systèmes de protection (firewall, IPS, UTM…). Inutile de dire qu'il n'est pas toujours apprécié des administrateurs. Mais pour un particulier, un groupe d'amateurs recherchant à la fois un programme de prise de contrôle à distance et un éventail d'outils capables de paramétrer la station distante, c'est l'outil idéal. Paradoxalement, un débutant adoptera ce programme avec la même facilité, en ignorant les gadgets techniques proposés par l'éditeur. L'usage de sessions d'assistance à distance à durée limitée restreint les risques d'intrusion. Mais l'on est obligé de croire l'éditeur sur parole lorsqu'il affirme que ses communications chiffrées sont fortement sécurisées (**www.logmein.com**). ■

CARACTÉRISTIQUES

Multiplateforme (Windows, Linux, Mac), pas de limitation du nombre de serveurs gérés, existe en version professionnelle avec fonctions évoluées (transfert de services, outils collaboratifs, réseau IP/Web)

VERDICT

Son interface graphique, son tableau de bord web et ses fonctions de déploiement de programmes en font un outil véritablement universel.

SIMPLICITÉ — RICHESSE FONCTIONNELLE — ERGONOMIE

NOTE 17/20

> ULTRAVNC ■ GRATUIT

Une porte d'entrée vers l'accès distant

C'est le 4x4 du remote control, ce VNC-là. Quelle que soit l'édition de Windows ou le parfum ésotérique d'un Linux austro-hongrois, VNC répond présent. Sa variante UltraVNC, également proche du « code originel » et respectueuse du projet initial, n'intègre pas par défaut de couche de chiffrement; ce qui n'interdit pas d'en ajouter une en option. Comparé à ses concurrents, il peut paraître bien pauvre en fonctionnalités. C'est la rançon de son universalité. L'avantage de cet aspect spartiate, c'est une empreinte mémoire insignifiante (2,7 Mo) et une réelle rapidité, notamment en application sur réseau local. Une version « VNC SC » (pour « single clic »), serveur sans installation de 300 Ko maximum, existe même pour les interventions au coup par coup (**www.ultravnc.com**). ■

CARACTÉRISTIQUES

Tous réseaux IP, toutes plateformes, pas de limitation du nombre de serveurs distants gérés, évolution récente client java pour les principaux navigateurs, fenêtre de discussion, module de cryptage Ultravnc.com

VERDICT

Un outil minimaliste mais pas « limité », réservé à ceux qui recherchent la légèreté et la simplicité. Il nécessite un chiffrement optionnel.

SIMPLICITÉ — RICHESSE FONCTIONNELLE — ERGONOMIE

NOTE 16/20

Release by TEAM-DZ

> TEAMVIEWER 6 ■ GRATUIT

Le démon de la démo

TeamViewer est véritablement le programme le mieux adapté aux démonstrations et sessions de formation/apprentissage à distance. Pour peu, ses modules de prise de contrôle à distance, de vidéo chat, de boot télécommandé ou d'échange de fichiers rapide passeraient au second plan. Tout comme son concurrent LogMeIn, il passe au travers des firewalls et des proxy-NAT avec une facilité déconcertante, propre à effrayer un administrateur… et à combler d'aise un usager qui ne maîtrise pas toutes les arcanes des réseaux locaux ou étendus. Sa version « portable » utilisant un navigateur web et les services de connexion de TeamViewer.com reste certes moins riche que celle de LogMeIn mais y gagne en simplicité d'utilisation. La gestion des mots de passe d'ouverture de session est intéressante… et unique. Qualité et rigorisme tout germaniques (**www.teamviewer.com**). ■

CARACTÉRISTIQUES

Toutes machines Microsoft : XP, Vista, Windows 7, ou 2003/2008/R2 sous Mac OSX, Linux et iPhone, pas de limitation du nombre de serveurs gérés, réseau IP/Web

VERDICT

Aussi agréable à utiliser sur un réseau local que via internet, son mode « démo/formation » en fait le programme idéal en cas d'urgence.

SIMPLICITÉ — RICHESSE FONCTIONNELLE — ERGONOMIE

NOTE 16/20

> BUREAU À DISTANCE (MICROSOFT)

Une fenêtre ouverte sur Windows

La fonction RDP (Remote Desktop Protocol), qu'elle aboutisse sur une console de serveur (console d'administration à distance) ou sur une station (Bureau à distance), ne fait que « rediriger » l'écran et le clavier du système télécommandé. Pratique pour prendre la main sur un Home Server ou la machine d'un réseau familial, c'est l'outil de prise de contrôle à distance pour tous ceux qui ne veulent pas installer d'outil de prise de contrôle à distance… L'emploi de ces « consoles distantes » exige la modification des règles de contrôle d'entrée du firewall. Son client RDP spécifique (client pour Bureau à distance) ou son mécanisme d'accès web (TS Web) s'adapte à toutes les situations. ■

CARACTÉRISTIQUES

Une à dix machines sous XP, Vista, Windows 7, ou 2003/2008/R2, réseau IP, protocole propriétaire Microsoft en réseau local

VERDICT

Simplicité extrême, grande versatilité, mais une certaine lourdeur en administration multiple et en paramétrage réseau.

SIMPLICITÉ — RICHESSE FONCTIONNELLE — ERGONOMIE

NOTE 15/20

distance », autorise les interactions entre les deux utilisateurs distants. Le mode démonstration donne à l'initiateur de la connexion le droit de « prendre la main » de manière exclusive sur l'application placée en « mode démo ». L'installation de TeamViewer ajoute un bouton supplémentaire dans la « caption barre » de toutes les applications Windows ; bouton qui démarre automatiquement le lancement du mode démonstration ou partage entre deux machines. Il est intéressant de noter que le mode démonstration/assistance n'utilise pas les mêmes mots de passe, et que la totalité des échanges est chiffrée en AES256. La liste des outils complémentaires est longue : client de vidéoconférence intégré, redémarrage et reconnexion automatique de la machine distante (une nécessité dans le cadre de toute assistance technique), optimisation de la qualité d'affichage en fonction de la bande passante disponible, annuaire des appareils accessibles à l'intérieur d'un « groupe TeamViewer ». Une possibilité de lancement en version « portable » (sans installation préalable) permet à une personne possédant un compte TeamViewer de déclencher une prise de contrôle à distance depuis un navigateur web, en transitant par le site TeamViewer.com. Accès protégé, l'on s'en doute, par un mot de passe et un login unique. Il faut chercher longtemps avant de trouver certains défauts. Ainsi, une station de contrôle très classique avec écran 4/3 a provoqué des problèmes d'affichage sur un client (hôte distant) doté d'un écran au format 16/9. La palette de couleurs n'était parfois pas fidèle… et l'usage en réseau local s'avérait plus lent que son concurrent Windows Remote Desktop – les performances sont comparables via internet. Outil « trop complet » pour ceux qui ne cherchent qu'un programme d'accès à distance, le nombre de paramètres à prendre en compte et de possibilités offertes pourrait, en effet, noyer un néophyte. Reste que pour un utilisateur averti, il ne faut pas plus de quinze minutes pour faire le tour du programme et en saisir toute la puissance !

LogMeIn : gratuit, simple et rapide

Si TeamViewer demeure le couteau suisse de la téléopération informatique, LogMeIn en est l'opinel. Tout aussi gratuit que son

Release by TEAM-DZ

ZOOM > Le tableau de bord DES COMMANDES À DISTANCE

concurrent, il ne prétend pas tout faire : un mode présentation, une fonction de partage de fichiers, une autre de partage de bureau. Mais la rapidité est au rendez-vous. Les demandes d'invitation à distance transitent par un service centralisé et ne sont pas sans rappeler le mode de fonctionnement des programmes de messagerie instantanée ou de téléphonie sur IP (invitation Skype, MSN Messenger, etc.). L'invité lance la session d'assistance à distance en activant une URL communiquée par e-mail : action à effectuer dans un laps de temps déterminé et précisé par le requérant. Les échanges de fichiers sont assurés par une extension spéciale, et comme son concurrent TeamViewer, l'accès aux machines équipées du logiciel s'avère possible depuis le site de l'éditeur (www.logmein.com). Une fois authentifié puis connecté à l'un des ordinateurs « logmeinisé », le service donne alors accès à un tableau de bord impressionnant qui ne se limite pas à une simple fonction d'écran déporté. Base de registre, gestion des journaux d'alerte, taux d'utilisation des ressources, statistiques fournies par Perfmon, « chat » d'assistance, partage et transfert de fichiers, métaphore du Gestionnaire de programmes indiquant les tâches en cours, taux d'occupation des disques… toute la gestion locale de la machine est là, à portée de souris. LogMeIn reste un outil pouvant trouver sa place aussi bien sur le système d'un débutant, cherchant à faire appel à un mentor distant, que dans l'arsenal d'un administrateur. Un administrateur qui, grâce à cette interface web, peut effectuer son travail depuis un Web café. Travail d'autant plus aisé que d'autres outils, également accessibles à partir de cette console d'administration, donnent accès au responsable d'un groupe d'ordinateurs, à des éditions de rapports statistiques, à des journaux d'événements consacrés aux opérations de prise de contrôle à distance, à la constitution et gestion de groupes de machines, à l'exécution distante d'un programme sur plusieurs systèmes ou au déploiement d'un exécutable.

UltraVNC, un ancêtre vigoureux…

Né du monde Linux, il y a fort longtemps, VNC est l'archétype des logiciels de prise de contrôle à distance. Universel, il a su se fondre totalement dans les environnements Windows et Macintosh, à tel point qu'Apple l'a intégré à son noyau « en standard ». La version Windows supporte aussi bien Windows 7 qu'un antique Windows 95. Et la console déportée utilise n'importe quel navigateur supportant Java. Tout comme ses concurrents, le programme possède son propre utilitaire de transfert de fichiers, mais son usage sur réseau public doit être soumis à quelques précautions d'usage. Par défaut, pour des raisons d'orthodoxie, VNC ne chiffre pas ses communications. Mais tout est prévu pour protéger les échanges avec le mécanisme de son choix… Ce qui, d'un point de vue technique, semble bien plus rassurant qu'un protocole prétendument inviolable mais maîtrisé par l'éditeur du programme, et lui seul. En option également, une fenêtre de « chat » nécessaire lors des sessions d'assistance et de maintenance. Pour le reste, VNC ne fait QUE de la redirection écran-clavier. Mais il le fait bien, de manière fiable, et depuis des décennies ! **Marc Olanié et Solange Belkayat**

L'AVIS DE L'EXPERT

Microsoft a développé une version « compacte » de son offre serveur, baptisée Small Business Server. Cette édition possède un outil très particulier et peu connu : le poste de travail Web à distance qui donne à tous les utilisateurs authentifiés le droit d'accéder à distance au réseau de la PME, à certaines applications et à quelques tâches administratives.

Release by TEAM-DZ

Astuces express

MATÉRIEL REQUIS
Office 2007 et 2010

NIVEAU
Facile

QUESTION

Vous avez besoin d'envoyer par e-mail des documents Office. Vous voudriez être sûr que vos contacts pourront les ouvrir et que la mise en page sera préservée. Dans quel format vaut-il mieux les enregistrer ?

Enregistrez vos documents Office au format PDF

> Word, Powerpoint et Excel À partir de n'importe quelle application Office 2007 ou 2010, cliquez sur le bouton *Office* ou *Fichier*. Puis, dans le menu qui s'affiche, choisissez la commande *Enregistrer sous*. Ouvrez la liste *Type* et sélectionnez *PDF*. Les options d'enregistrement varient selon l'application. Pour un document Word, choisissez les pages. Vous pouvez également en profiter pour convertir les titres ou les signets Word en signets PDF. Ceux-ci seront utilisés dans le lecteur PDF pour faciliter les déplacements rapides dans le document. Pour un classeur Excel, vous pouvez limiter l'enregistrement à la page ou aux feuilles sélectionnées. Pour une présentation Powerpoint, vous choisissez les diapositives à indure, le nombre de dias par page, l'ajout des commentaires, l'insertion du plan. Si vous voulez présenter le document PDF sur un site ou un blog, vous avez intérêt à ce qu'il soit le plus léger possible. Cochez l'option *Taille minimale*. Cette option agit principalement sur les images qui sont compressées et donc de moins bonne qualité. Lorsque vous cliquez sur le bouton *Enregistrer*, le document PDF est généré et immédiatement ouvert dans le lecteur approprié (généralement Adobe Reader). Si ce logiciel n'est pas installé sur votre PC, téléchargez-le et installez-le : **www.adobe.com/fr/products/reader**. Il est gratuit.

MATÉRIEL REQUIS
Internet

NIVEAU
Facile

QUESTION

Votre PC semble trop lent et, malgré votre antivirus, vous soupçonnez une infection par des spywares. Que faire pour résoudre le problème ?

Procédez à un test antimalware gratuit sur internet

> Accédez à l'outil d'analyse Entrez dans votre navigateur l'adresse www.pandasecurity.com/activescan. Sélectionnez l'analyse rapide (elle dure quelques minutes mais n'examine que les éléments critiques) ou l'analyse complète (elle examine tout le système mais peut durer plusieurs heures). Cliquez sur *Analyser*.

> Téléchargez le plug-in ActiveScan a besoin d'un module complémentaire ou d'un contrôle ActiveX pour fonctionner. Acceptez son installation et suivez les instructions. Autorisez l'exécution des fichiers provenant de Panda Security. Une fois l'analyse terminée, ActiveScan affiche les menaces, virus et logiciels espions détectés.

> Une analyse personnalisée Si vous cliquez sur *Conseil de désinfection*, vous serez invité à acheter l'antivirus Panda, ce qui n'est pas obligatoire. Dans la page d'accueil d'ActiveScan, cliquez sur *Autres analyses*. Vous pouvez alors choisir parmi trois types d'analyse : les documents, les e-mails ou les éléments que vous choisissez vous-même.

1

2

3

Release by TEAM-DZ

WINDOWS
PUIS-JE RETIRER LA CLÉ USB ?

Q ***Quand je clique sur l'icône qui permet de retirer un périphérique en toute sécurité, la fenêtre qui indique « Le périphérique peut être retiré en toute sécurité » n'apparaît plus !***

De Luc Bénegent

R Cette icône ne demeure pas vraiment indispensable. Si vous retirez le périphérique (une clé USB, par exemple) pendant le transfert d'un fichier, celui-ci sera endommagé et très certainement illisible. Il reste même possible qu'il faille reformater la clé. En cliquant sur l'icône, Windows contrôle qu'aucun transfert n'est en cours avant de vous donner l'autorisation de retirer le périphérique. Il n'y a aucun risque réel à déconnecter un périphérique sans passer par cette icône. Attendez simplement quelques secondes après avoir copié un fichier sur le périphérique.
Si vous voulez quand même que Windows contrôle le retrait des périphériques USB, créez un raccourci sur le Bureau. Faites comme ceci : cliquez du bouton droit sur le Bureau et choisissez la commande *Nouveau > Raccourci*. Dans la boîte de dialogue, entrez la commande *rundll32.exe shell32.dll, Control_RunDLL hotplug.dll*. Cliquez sur *Suivant* et entrez le nom qui sera attribué à l'icône. Un double-clic sur celle-ci ouvre alors la boîte de dialogue *Supprimer le périphérique en toute sécurité*. ■

SKYPE
ON NE M'ENTEND PAS

Q ***Lors des communications audio avec Skype, j'entends parfaitement mes contacts mais eux ne m'entendent pas !***

De Daniel Tissaud

R Vérifiez le bon fonctionnement de votre micro. Trois points sont à contrôler. Un : ouvrez le module *Son* ou *Sons et périphériques audio* du Panneau de configuration. Dans l'onglet *Enregistrement*, contrôlez si le micro reste coché. S'il ne l'est pas, cochez-le ou double-cliquez dessus pour l'activer. Deux : dans la fenêtre de Skype, choisissez la commande *Outils > Options* et cliquez sur la catégorie *Paramètres audio*. La liste Microphone affiche le nom de votre micro. Cochez l'option *Laisser Skype gérer mes paramètres audio*. Trois : mettez à jour le pilote de la carte son. Ouvrez le Gestionnaire de périphériques et double-cliquez sur le nom de la carte son. Notez le nom du fabricant et le modèle de la carte.
Rendez-vous sur le site www.touslesdrivers.com pour trouver facilement la page concernant le pilote de votre carte son. Téléchargez et installez le pilote le plus récent adapté à votre version de Windows. ■

WINDOWS
LA SOURIS RÉVEILLE LE PC

Q ***Quand mon PC est en veille, le moindre mouvement de la souris le réactive. Je préférerais qu'il sorte de veille lorsque je presse une touche du clavier.***

De Gilles Desruelle

R Ouvrez le Gestionnaire de périphériques et double-cliquez sur le nom de la souris. Dans la fenêtre de ses propriétés, passez à l'onglet *Gestion de l'alimentation*. Décochez l'option *Autoriser ce périphérique à mettre l'ordinateur en éveil* ou (si vous avez Windows 7) *Autoriser ce périphérique à sortir l'ordinateur du mode veille*. Validez avec *OK*. Double-cliquez ensuite sur le nom du clavier. Vous trouverez la même option dans le même onglet de la fenêtre de ses propriétés. Vérifiez qu'elle soit bien cochée. ■

OUTLOOK
SYNCHRONISEZ OUTLOOK SUR DEUX ORDINATEURS

Q ***Je possède un PC de bureau et un portable. J'utilise Microsoft Outlook et je voudrais synchroniser les données d'Outlook sur les deux PC (calendrier, e-mails, tâches).***

De Fabrice Ridelle

R Outlook stocke toutes les données dans un unique fichier. Pour connaître son nom et son emplacement, cliquez du bouton droit dans la fenêtre d'Outlook sur *Dossiers personnels* et choisissez la commande *Propriétés du fichier de données*. Cliquez ensuite sur le bouton *Options avancées* : le nom du fichier se trouve là. Vous pouvez alors copier manuellement ce fichier d'une machine à l'autre. Le fichier ne porte pas nécessairement le même nom sur les deux ordinateurs. Supposons que ce fichier se nomme bobby.pst sur le PC de bureau et paul.pst sur l'ordinateur portable ; procédez alors comme ceci : fermez Outlook sur les deux machines puis par l'intermédiaire de votre réseau local, copiez le fichier bobby.pst depuis le PC sur le portable (dans le dossier où se trouve déjà paul.pst). Sur l'ordinateur portable, supprimez paul.pst et renommez bobby.pst en paul.pst.
Par sécurité, plutôt que de supprimer paul.pst, renommez-le par exemple paul.old. Cette solution s'avère un peu lourde, il est vrai. Il existe un logiciel de synchronisation automatique : OsaSync Pro (www.vaita.com/index_fr.asp). Sa licence coûte 59,95 euros. Si vous voulez synchroniser uniquement les contacts sur quatre ordinateurs maximum, la version Lite (gratuite) est suffisante. ■

Tous les mois Jean-Paul Mesters répond à vos questions
hotline.wnews@yellowmedia.fr

HOTLINE

Journaliste, Jean-Paul Mesters est l'auteur d'une trentaine d'ouvrages d'informatique grand public. Il gère le site web Docmemo.

WINDOWS
PLUS DE COMMANDE

Q ***La commande* Envoyer vers > Destinataire *a disparu du menu contextuel des fichiers et des dossiers. Comment la restaurer ?***

R Commencez par demander l'affichage des fichiers et dossiers cachés. Ouvrez l'Explorateur Windows. Si vous avez Windows 7 ou Vista, cliquez sur *Organiser* puis sur *Options des données et de recherche*. Avec Windows XP, choisissez la commande *Outils > Options des données et de recherche*. Dans l'onglet *Affichage de la fenêtre Options des dossiers*, cochez *Afficher les fichiers et dossiers cachés*. Décochez l'option *Masquer l'extension des fichiers dont le type est connu*. Si vous avez Vista ou Windows 7, ouvrez ensuite le dossier *C:\Utilisateurs\(nom)\AppData\Roaming\Microsoft\Windows\SendTo*. Si vous avez XP, ouvrez le dossier *C:\Documents and Settings\(nom)\SendTo*. Dans ce dossier, créez un fichier texte vide et nommez-le *Destinataire.MAPIMail*. Les autres éléments de ce dossier fonctionnent selon le même principe. Les fichiers se nomment Bureau(raccourci).DeskLink, DossierCompresse.ZFSendToTarget, Mes documents.MyDocs. ■

Release by TEAM-DZ

WINDOWS VISTA ET 7

AFFICHEZ LES GADGETS

Q ***Quand je veux afficher les gadgets sur le Bureau de mon ordinateur Vista, un message m'annonce que le volet Windows est géré par l'administrateur système. Je ne peux donc pas utiliser ces gadgets !***

De D. Pluvier

R Lancez *Regedit*. Dans la fenêtre de l'éditeur du registre, sélectionnez la clé *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar*. Double-cliquez sur *TurnOffSidebar* et entrez la donnée *0*. Attribuez également la donnée 0 à la valeur portant le même nom située sous la clé HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\Sidebar. ■

WINDOWS

NETTOYEZ LE SYSTÈME

Q ***J'utilise Vista depuis plusieurs années et tout se déroule à peu près bien… Il se passe cependant parfois quelques bugs et petites erreurs de Windows, et notamment des blocages sur internet. J'aimerais savoir s'il existe un logiciel fiable pour corriger Vista sans avoir à tout réinstaller ?***

De Gérard Creux

R Le logiciel gratuit CCleaner nettoie en profondeur et optimise le système. Téléchargez-le à partir de la page www.piriform.com/download. La fenêtre de CCleaner contient plusieurs outils. Le nettoyeur agit sur le système : il vide la poubelle, supprime les fichiers du dossier temporaire, les bouts de fichiers incomplets, les fichiers log. Lancez la recherche en cliquant sur le bouton *Analyser* : CCleaner affiche la liste des fichiers correspondant à votre demande. Vérifiez-la et lancez le nettoyage. Le bouton *Analyser* et le nettoyage lui-même agissent sur les éléments cochés dans les deux onglets : Windows et Applications. Passez ensuite au Registre. Cette section tout entière est réservée à la Base de registre. C'est là que se trouve l'origine de nombreux bugs et problèmes. La Base de registre réparée, prenez des précautions pour éviter les fausses manœuvres. Cochez les éléments qui vous semblent importants et lancez la recherche des erreurs. Une fois la liste générée par CCleaner, cliquez sur le bouton *Réparer les erreurs sélectionnées*. Un message vous propose de sauvegarder les changements. Acceptez. Un fichier portant l'extension reg est créé. En cas de problème, il suffit de double-cliquer sur son icône pour annuler les modifications au registre. Ensuite, une nouvelle fenêtre s'ouvre : elle passe en revue chaque erreur et affiche une explication détaillée. Cliquez sur *Corriger l'erreur* pour appliquer la solution indiquée. Pour passer à l'erreur suivante sans réparer, cliquez sur la double flèche. Pour traiter tous les problèmes rapidement, cliquez sur le bouton *Corriger toutes les erreurs sélectionnées*. Avant toute opération de nettoyage, créez un point de restauration. ■

MATÉRIEL

UTILISEZ UN SSD

Q ***Je viens d'acquérir un SSD de 120 Go. Malheureusement, il n'est pas reconnu par Windows 7. Il apparaît au démarrage de mon PC dans la liste des disques mais je ne le vois pas dans l'Explorateur Windows.***

De Hubert Ragaches

R Pour que Windows reconnaisse un SSD (tout comme un disque dur), il faut obligatoirement l'initialiser et le formater. Dans le Panneau de configuration, ouvrez le module *Outils d'administration* et double-cliquez sur *Gestion de l'ordinateur*. Dans le volet gauche de la fenêtre qui s'ouvre, cliquez sur *Gestion des disques*. Créez une partition sur le SSD et formatez-la : les commandes se trouvent dans le menu contextuel du disque. Le SSD est ainsi identifié par une lettre de lecteur. Utilisez-le pour stocker vos fichiers comme n'importe quel disque. Il ne faut jamais le défragmenter : ça diminuerait sa durée de vie. Sur un SSD, les données sont effacées dès que vous supprimez un fichier. Cette fonction, nommée TRIM est gérée par la plupart des SSD et contrôlée dans Windows 7. ■

MATÉRIEL

PÉRIPHÉRIQUES EN MANQUE D'ÉNERGIE

Q ***J'ai un concentrateur USB. Je le branche sur mon PC qui le détecte et l'installe. Je connecte sur ce concentrateur une imprimante et un scanner. Au bout de cinq minutes environ, les voyants où sont branchés l'imprimante et le scanner s'éteignent et ne répondent plus. Je suis obligé de débrancher puis de rebrancher le concentrateur pour que ça fonctionne à nouveau pendant quelques minutes.***

De Alain Noiré

R Windows, pour des raisons d'économie, désactive parfois les périphériques USB restés trop longtemps inactifs. Les concentrateurs USB (tout comme les ports USB) ont en effet besoin d'énergie pour fonctionner. Cette électricité est fournie par l'alimentation du PC. Pour l'économiser, la plupart des concentrateurs ont leur propre alimentation électrique. De cette manière, Windows ne sera plus tenté de mettre hors service les périphériques USB. Si le problème n'est pas résolu, branchez l'un des deux périphériques directement sur un port USB et non pas sur le concentrateur. La consommation sera ainsi mieux répartie. Si Windows continue à désactiver les périphériques, opérez ainsi : si vous avez Windows XP, ouvrez le module *Système* du Panneau de configuration. Dans l'onglet *Matériel*, cliquez sur le bouton *Gestionnaire de périphériques*. Avec Windows 7 ou Vista, ouvrez directement le module *Gestionnaire de périphériques*. Dans la catégorie Contrôleurs de bus USB, vous voyez alors une liste de concentrateurs. Pour savoir lequel correspond au périphérique en cause, double-cliquez sur chacun d'eux et passez à l'onglet *Marche/Arrêt* où vous voyez le nom des périphériques qui lui sont attachés. Lorsque vous avez trouvé le concentrateur qui gère le périphérique, cliquez sur l'onglet *Gestion de l'alimentation* et décochez l'option *Autoriser l'ordinateur à éteindre ce périphérique* pour économiser l'énergie. ■

Release by TEAM-DZ

WINDOWS 7 ET VISTA

UNE EXTENSION OUBLIÉE

Q ***J'ai reçu par e-mail un fichier avec l'extension eml que je n'ai pas pu ouvrir. Windows m'informe qu'aucun programme n'est attaché à cette extension. Dans le module* Programmes par défaut *du Panneau de configuration, je ne retrouve pas .eml !***

De Raymond Blois

R Lorsqu'on insère un e-mail dans un message, le fichier joint porte l'extension eml. Un double-clic sur ce fichier suffit pour ouvrir le message avec votre logiciel de messagerie habituel (Outlook, Windows Live Mail, etc.). Votre premier réflexe est le bon : vérifiez dans le module Programmes par défaut du Panneau de configuration à quel logiciel l'extension .eml est associée. Vous pouvez cliquer sur *Changer le programme* pour corriger ou rétablir l'association. Si l'extension reste absente de la liste dans ce module, il faut aller voir dans la Base de registre. Ouvrez-la avec son éditeur regedit. Les extensions sont référencées dans la branche HKEY_CLASSES_ROOT. Sous la clé .eml, vous devriez voir normalement trois sous-clés : OpenWithProgids, PersistentHandler et ShellEx. Pour que Windows gère correctement cette extension, prenez exemple sur l'extension .msg dans cette même branche. Les trois sous-clés de l'extension .eml et leurs valeurs doivent être identiques à celles de .msg. Reconstituez la clé .eml en prenant pour exemple la clé .msg. ■

MULTIMÉDIA

CODAGE AUDIO DANS UNE VIDÉO

Q ***J'enregistre sans problème les chaînes TV SD. En revanche, pour les films des chaînes HD, je n'arrive pas à décoder le son qui est au format E-AC3. Comment transformer la piste son E-AC3+ en AC3 tout en gardant la vidéo H264 en HD ?***

De Thierry Grollier

R Beaucoup d'utilisateurs ne peuvent pas lire les enregistrements TNT HD. Leur logiciel ou leur boîtier multimédia ne sont pas compatibles avec le format sonore Dolby Digital Plus (E-AC3). La France est l'un des seuls pays en Europe à utiliser ce format sonore à la télévision et donc peu de constructeurs se donnent la peine de payer les licences Dolby pour l'E-AC3. Heureusement, il existe un logiciel français gratuit qui effectue cette conversion : m4ng (www.m4ng.fr). À partir de la page d'accueil du site, téléchargez puis installez le pack de codecs ainsi que Video Enhancer. Pour convertir la piste audio en AC3, lancez *Video Enhancer* et commencez par démixer le son et la vidéo. Renommez ensuite le fichier audio en remplaçant l'extension .ac3 en .eac3. Enfin, remixez le son et la vidéo. ■

WINDOWS

VERROUILLAGE NUMÉRIQUE

Q ***Quand je démarre mon PC, le pavé numérique du clavier n'est pas activé. Je suis obligé de presser chaque fois la touche [Verr Num]. Comment faire pour que le pavé numérique soit activé au démarrage de Windows ?***

De Sylvain Bigaud

R Lancez *regedit*, l'éditeur de la Base de registre et sélectionnez la clé *HKEY_CURRENT_USER\Control Panel\Keyboard*. Double-cliquez sur la valeur *InitialKeyboardIndicators* et entrez la donnée 2. Cette valeur accepte les données suivantes : 0 (Verr Num, Blocage majuscules et Arrêt défilement off), 1 (Blocage majuscules on), 2 (Verr Num on), 3 (Blocage maj. et Verr Num on), 4 (Arrêt défil. on), 5 (Blocage maj. et Arrêt défil. on), 6 (Arrêt défil. et Verr Num on), 7 (Blocage maj., Verr Num et Arrêt défil. on). ■

WINDOWS

LES POINTS DE RESTAURATION DISPARAISSENT

Q ***J'ai installé Windows 7 en dual boot avec Windows XP. Les points de restauration disparaissent systématiquement.***

De Jacques Vielfaure

R Ouvrez une session Windows XP. Dans le Poste de travail, notez les lettres des lecteurs sur lesquels sont installés les OS. Par exemple : C pour XP et E pour Windows 7. Lancez *regedit*, l'éditeur de la Base de registre, et sélectionnez la clé *HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices*. Choisissez la commande *Édition > Nouveau > Clé*. Nommez la clé *Offline* et sélectionnez-la. Choisissez ensuite la commande *Édition > Nouveau > Valeur DWORD*. Nommez cette valeur *\DosDevices\E:* (puisque le lecteur où est installé Vista porte la lettre E). Double-cliquez sur la valeur et attribuez-lui comme donnée *1*. Fermez *regedit*. Ensuite, dans le Panneau de configuration, ouvrez le module *Système* et dans la fenêtre passez sous l'onglet *Restauration du système*. Veillez à ce que le lecteur C (là où est installé XP) soit sous surveillance. Sélectionnez le lecteur E. Cliquez sur *Paramètres* et désactivez la restauration du système sur ce lecteur. Redémarrez le PC sous XP pour que les modifications soient activées. Redémarrez le PC sous Windows 7. Ouvrez le module *Système* du Panneau de configuration et cliquez sur *Protection système*. Vérifiez que la protection est active uniquement sur le volume où W7 est installé. ■

HOTLINE

MESSAGERIE

MAL INSTALLÉ...

Q ***J'ai mis en place Windows Live Mail. À la fin de l'installation, le message d'erreur suivant s'affiche : « le composant que vous essayez d'utiliser se trouve sur une ressource réseau non disponible ». Ce message apparaît maintenant régulièrement.***

De Philippe Martin

R Désinstallez puis réinstallez Windows Live Mail. Mais avant tout, lancez une copie de sécurité des messages. Pour savoir où ils sont situés, choisissez la commande *Outils > Options* dans la fenêtre de Windows Mail. Passez à l'onglet *Avancé* et cliquez sur *Maintenance*. Dans la fenêtre Maintenance, cliquez sur le bouton *Dossier de stockage*. Ouvrez ensuite l'Explorateur Windows et sélectionnez ce dossier pour en faire une copie sur le Bureau, par exemple. Faites également une copie des comptes de messagerie. Choisissez la commande *Outils > Comptes*. Sélectionnez les comptes un à un et pour chacun, cliquez sur le bouton *Exporter*. Désinstallez Windows Live Mail puis réinstallez Windows Mail. Recopiez les messages dans le dossier où vous les avez trouvés. Et enfin, récupérez les comptes que vous avez sauvegardés : dans la fenêtre de la commande *Outils > Comptes*, cliquez sur *Importer*. ■

Release by TEAM-DZ

MATÉRIEL
MÉMOIRE INUTILISABLE

Q ***J'ai ajouté de la mémoire vive dans mon ordinateur mais Windows 7 ne la reconnaît pas. Il affiche « Mémoire installée 8 Go, utilisable 2,99 Go ».***

De Yves Le Gall

R Que la quantité de mémoire utilisable soit inférieure à la mémoire installée, c'est normal. En effet, la mémoire utilisable dépend de plusieurs facteurs. Windows en version 32 bits ne gère pas plus de 3 Go. Vérifiez également que la quantité de mémoire gérable par le système n'est pas bridée. Cliquez sur le bouton *Démarrer*, tapez *msconfig* et pressez la touche [Entrée]. Dans la fenêtre de configuration du système, passez à l'onglet *Démarrer* et cliquez sur *Options avancées*. L'option *Mémoire maximale* doit être désactivée. Autre piste de solution : le Bios. Visitez le site web du fabricant pour télécharger la mise à jour la plus récente et suivez les instructions pour l'installer. Enfin, assurez-vous que les barrettes de mémoire sont en bon état et que leur modèle est reconnu par la carte mère (reportez-vous au mode d'emploi). ■

SÉCURITÉ
DÉSINSTALLATION

Q ***J'essaie de désinstaller Norton 360. À chaque essai, le message suivant s'affiche : « Une erreur s'est produite lors de la désinstallation de Norton 360 ».***

De Guy Troquat

R Symantec fournit gratuitement un utilitaire de désinstallation de ses logiciels. Pour le trouver, rendez-vous à l'adresse www.symantec.com/fr/fr/norton/support/index.jsp. Cliquez dans cette page sur *Support technique*. Ensuite, ouvrez la liste des produits pour choisir *Norton 360*, sélectionnez le numéro de version dans la seconde liste et cliquez sur *Continuer*. Dans la page du support technique, lancez une recherche sur *Outil de suppression*. Dans la liste des résultats, faites un clic sur *Télécharger et exécuter l'outil de suppression Norton*. Dirigez-vous enfin sur le bouton *Télécharger*. Une fois le fichier sur votre PC, double-cliquez sur son icône (il se nomme Norton Removal Tool). Dans le message qui apparaît, choisissez *Setup*. Il vous reste à cliquer sur quelques boutons *Suivant* pour que l'utilitaire fasse son travail. ■

MATÉRIEL
BOOTEZ SUR UN SSD

Q ***Je veux remplacer mon disque de démarrage C par un SSD. J'ai également un disque D sur lequel j'ai stocké uniquement des photos.***

De Éric Chazeau

R Avant de vous répondre, un petit rappel : un SSD (Solid State Disk) est un composant matériel constitué de mémoire Flash, destiné au stockage de fichiers. Un SSD a les mêmes fonctions qu'un disque dur mais le temps d'accès est beaucoup plus court (0,1 ms au lieu de 13 ms) et le débit en lecture et écriture, plus élevé. En outre, puisqu'il ne renferme aucune pièce mécanique, il demeure parfaitement silencieux. Les SSD sont généralement fournis avec un utilitaire de clonage pour le transfert du contenu intégral d'un disque dur. Étant donné leur prix encore élevé, ceux que vous achèterez seront probablement de capacité inférieure à celle du disque dur. Avant d'installer un SSD, transférez vos données du lecteur C vers un autre disque. Il faudra peut-être aussi désinstaller quelques logiciels. Objectif : l'espace utilisé sur le lecteur C ne doit pas dépasser la capacité du SSD. Éteignez ensuite l'ordinateur. Connectez le SSD au PC avec le câble de transfert USB. Insérez le CD fourni dans le lecteur et démarrez le PC à partir du CD. Suivez les instructions pour cloner le lecteur C sur le SSD. Une fois le clonage terminé, éteignez l'ordinateur et ouvrez son capot pour retirer le disque dur et installer le SSD. Redémarrez le PC. L'ancien disque peut être réutilisé pour le tockage de données, par exemple. ■

WINDOWS
REFUS DE LECTURE

Q ***Chaque fois que j'introduis un CD ou DVD vierge, le système affiche un écran bleu avec des informations que je ne peux pas lire car le système redémarre. Est-ce un problème de compatibilité matérielle ? J'utilise Windows Vista.***

De Dominique Prigeant

R L'écran bleu signifie qu'une erreur fatale s'est produite. Pour prendre connaissance du code et de l'explication de l'erreur, empêchez Windows de redémarrer automatiquement. Ouvrez le module *Système* du Panneau de configuration. Dans le bandeau gauche de la fenêtre, cliquez sur *Paramètres du système avancé*. Dans la fenêtre des propriétés système, activez l'onglet *Paramètres système avancé*. Cliquez ensuite sur le bouton *Paramètres du cadre Démarrage et récupération*. Décochez l'option *Redémarrer automatiquement* et validez avec *OK*. Lorsque l'écran bleu apparaîtra à nouveau, notez le code de l'erreur. Il se présente comme ceci : 0x suivi de 8 chiffres ou lettres. Par exemple : 0x000000C1. Voyez sur DOCmémo la signification de ce code et les suggestions de solutions pour résoudre le problème : www.docmemo.com/windows/erreursstop.php. ■

Release by TEAM-DZ

OFFICE 2007

OÙ EST PERSO.XLS ?

Q ***Je viens de récupérer un portable qui dispose d'Excel 2007. Avec les versions antérieures, c'est dans le fichier perso.xls qu'on enregistrait les macros disponibles au démarrage. Comment faire avec Excel 2007 ?***

De Bernard Baillon

R Avec Excel 2007 et 2010, le fichier se nomme personal.xlsb. Pour s'ouvrir au démarrage d'Excel, il doit se trouver dans le dossier C:\Documents and Settings\(nom)\Application Data\Microsoft\Excel\XLSTART (XP) ou C:\Users\(nom)\AppData\ Roaming\Microsoft\ Excel\XLSTART (Windows 7 ou Vista). À l'installation d'Office, les macros ne sont pas transférées dans personal.xlsb. Il faut le faire manuellement par un copier/coller. ■

MULTIMÉDIA

NETTOYEZ LA BIBLIOTHÈQUE

Q ***Lorsque je complète la liste des dossiers à surveiller, le lecteur Windows Media complète la bibliothèque automatiquement chaque fois que de nouveaux fichiers sont introduits. En revanche, lorsque je retire un dossier de cette liste, les fichiers qu'il contient restent dans la bibliothèque. Je peux effacer les titres un à un, mais c'est fastidieux !***

De Roland

R Pour rappel, la liste des dossiers à surveiller est accessible comme ceci : cliquez sur la flèche située sous le gros bouton Bibliothèque. Dans le menu, choisissez la commande *Ajouter à la bibliothèque*. Dans la fenêtre qui s'ouvre, cliquez sur le bouton *Options avancées*. Vous avez accès à la liste des dossiers surveillés par le lecteur. Vous pouvez ajouter ou supprimer des dossiers. Puisque le lecteur ne tient pas compte de la suppression des dossiers de cette liste, il faut lui imposer la recréation de la bibliothèque. Malheureusement, aucune commande n'est prévue. La procédure reste donc un peu compliquée. Commencez par activer l'affichage des fichiers cachés. Avec Windows XP, ouvrez le Poste de travail et choisissez la commande *Outils > Options des dossiers*. Avec Windows Vista ou 7, ouvrez le dossier *Ordinateur* et choisissez la commande *Organiser > Options des dossiers et de recherche*. Dans les deux cas, la boîte de dialogue Options des dossiers s'ouvre. Passez à l'onglet *Affichage* et cochez l'option *Afficher les fichiers et dossiers cachés*. Validez avec *OK*. Fermez le lecteur Windows Media. Ouvrez ensuite le dossier où est stockée la bibliothèque du lecteur. Vous pouvez passer par l'Explorateur Windows, mais ce n'est pas indispensable. Avec Windows XP, cliquez sur le bouton *Démarrer* puis sur *Exécuter*. Tapez *%userprofile%\Local Settings\Application Data\Microsoft\Media Player* et pressez la touche [Entrée]. Avec Windows Vista ou 7, cliquez sur *Démarrer* puis dans la zone *Rechercher* et tapez *%LOCALAPPDATA%\Microsoft\Media Player*. Supprimez tous les fichiers que vous trouvez dans ce dossier, mais ne touchez pas aux sous-dossiers. Relancez Windows Media Player : il reconstruit la bibliothèque en fonction de la liste des dossiers à surveiller. Cette procédure s'avère également utile dans le cas où le lecteur refuse de démarrer en annonçant que la bibliothèque est endommagée. ■

PÉRIPHÉRIQUES

MAUVAIS FONCTIONNEMENT

Q ***Dans le Gestionnaire de périphériques, certains éléments affichent un point d'exclamation jaune. Par exemple : carte Microsoft ISATAP. J'ai mis à jour le pilote, mais la marque reste. Est-ce normal ?***

De Jean Chimien

R Cette marque indique généralement la présence d'un problème. Double-cliquez sur le nom de l'élément. La fenêtre de ses propriétés s'ouvre : l'onglet Général affiche l'état du périphérique et décrit le problème. Souvent, c'est le pilote qui est en cause parce qu'il n'est adapté ni au périphérique, ni à votre version de Windows. Installez un pilote plus récent en passant par www.touslesdrivers.com, qui facilite l'accès à la page de téléchargement des pilotes sur le site du fabricant. Chez vous (comme chez la plupart des utilisateurs), la carte Microsoft ISATAP est marquée du point d'exclamation jaune. Ce périphérique ISATAP (inter Site Automatic Tunneling Address Protocol) n'est pas une vraie carte. Il s'agit plutôt d'un module logiciel qui aide les entreprises à passer en douceur du protocole Internet IPv4 à IPv6. Le problème de la carte Microsoft ISATAP est sans importance. N'en tenez pas compte : cela n'a aucune influence sur votre PC ni sur votre connexion internet. ■

WINDOWS XP

XP SUR UN DISQUE SATA

Q ***Je voudrais réinstaller Windows XP sur un disque dur Sata. Dans le courrier des lecteurs d'un précédent numéro, il est indiqué de copier le pilote Sata sur une disquette, mais mon PC n'a pas de lecteur de disquettes !***

De Bernard Venis

R L'installation de Windows XP sur disque Sata n'est pas facile, car cette version de Windows n'inclut pas les pilotes Sata. La procédure d'installation autorise la mise en place de pilotes étrangers, mais ceux-ci doivent être sur une disquette. Puisque vous n'avez pas de lecteur de disquettes, créez un nouveau CD Windows XP en y intégrant les pilotes. Commencez par télécharger les pilotes Sata de la carte mère. Rendez-vous sur le site du fabricant et téléchargez les pilotes correspondant au modèle exact de votre carte mère. Décompressez l'archive téléchargée et déplacez les fichiers sur le Bureau. Téléchargez ensuite l'utilitaire nLite (www.nliteos.com/download.html). Après son installation, démarrez-le. Première étape : choisissez le français. Étape suivante : indiquez le lecteur dans lequel vous avez inséré le CD de Windows, puis l'emplacement où nLite créera le Windows XP modifié (par exemple, un dossier nommé XP Sata sur le Bureau). Le logiciel copie le contenu du CD Windows dans ce dossier. Optez ensuite pour la gravure automatique et pour un ISO bootable. Dans la fenêtre de sélection des tâches, cliquez sur le bouton *Pilotes* puis sur *Insérer*. Sélectionnez le fichier *.inf* dans le dossier contenant le pilote sur le Bureau. Cliquez sur *Suivant* puis sur *Finaliser le processus*. Voilà ! Le pilote Sata est intégré. Gravez le contenu du dossier contenant Windows modifié (XP Sata dans notre exemple). Installez Windows avec ce nouveau CD. ■

Release by TEAM-DZ

WINDOWS LIVE
DÉSINSTALLATION

Q ***Il y a un mois, j'ai installé Galerie de photos Windows Live. Après des essais et l'utilisation de cet utilitaire, je m'aperçois qu'il monopolise beaucoup de ressources et donc ralentit assez fortement mon système. J'aimerais le désinstaller mais je n'y arrive pas.***

De Noël Caladors

R L'installation et la désinstallation des programmes Windows Live sont gérées par une application unique. Ouvrez dans le Panneau de configuration le module *Programmes et fonctionnalités* (Windows 7 ou Vista) ou le module *Ajout/Suppression de programmes* (Windows XP). Dans la liste des programmes, recherchez Windows Live Essentials et cliquez sur le bouton *Modifier*. Si Windows Live Essentials n'est pas dans la liste, procédez ainsi : ouvrez dans l'Explorateur Windows le dossier *C:\Program Files\Windows Live\installer* et double-cliquez sur l'icône du fichier wlarp.exe. La fenêtre qui s'ouvre propose de désinstaller ou de réparer les programmes Windows Live. Optez pour la désinstallation et cliquez sur le bouton *Continuer*. Cochez *Galerie de photos* et cliquez sur le bouton *Continuer*. ■

MATÉRIEL
ABSENCE DE SIGNAL VIDÉO

Q ***J'ai mis à jour le pilote de la carte graphique. Depuis, le message « No signal input » s'affiche et l'écran reste noir même après le redémarrage du PC !***

De Jean-Pierre Smidt

R Il est probable que le pilote ne convient pas à la carte graphique. La carte n'envoie plus d'image à l'écran : le message affiché signifie qu'il ne reçoit aucun signal vidéo. Pour résoudre ce problème, il faut restaurer l'ancien pilote. La solution, c'est le mode sans échec. Redémarrez l'ordinateur et, dès l'apparition des premiers messages, enfoncez la touche [F8]. Le menu de démarrage s'affiche. Tapez le numéro de l'option correspondant au mode sans échec. Ouvrez normalement la session Windows. Le Bureau est graphiquement très laid. C'est normal : Windows a mis en place un pilote générique qui n'est pas du tout performant, mais fonctionne avec toutes les cartes graphiques. Ouvrez le Gestionnaire de périphériques en cliquant directement sur l'icône de son module dans le Panneau de configuration (avec Windows Vista) ou en passant par le module Système (avec Windows XP). Dans la liste des périphériques, double-cliquez sur le nom de la carte graphique. La fenêtre de ses propriétés s'ouvre. Passez à l'onglet *Pilote* et cliquez sur le bouton *Version précédente*. Après la réinstallation de l'ancien pilote, quittez Windows et redémarrez normalement le PC. ■

VIDÉOS
LECTEUR WINDOWS MEDIA EN PANNE

Q ***Depuis une mise à jour sur mon portable Windows Vista, je ne peux plus visionner de vidéos avec le lecteur Windows Media. Il est pourtant bien présent dans le menu Démarrer mais n'est pas visible dans le module Programmes et fonctionnalités du Panneau de configuration. Je ne peux donc pas le désinstaller ou corriger son installation.***

De Jean Dormain

R Le lecteur Windows Media est complètement incorporé au système et Microsoft n'a pas laissé la possibilité de le désinstaller ni même de le réinstaller. Le centre de téléchargement en ligne ne propose pas la version 11 pour Windows Vista. Donc, en cas de problème, il n'y a que deux solutions : restaurer le système à une date où le lecteur était encore opérationnel ou réinstaller complètement Windows Vista. Il existe une troisième solution : oublier ce lecteur pour le remplacer par un autre. VLC, par exemple, est une très bonne alternative car plus complet et plus stable que le lecteur Windows Media. Il lit tous les formats vidéo y compris WMV, le format signé Microsoft. Téléchargez-le ici : www.videolan.org/vlc. ■

WINDOWS
UNE APPLICATION SUSPECTE

Q ***Au démarrage de mon ordinateur, entre l'apparition du bureau et celle du volet Windows, le message suivant s'affiche : « qsyko.exe a cessé de fonctionner ». De quoi s'agit-il ?***

De Michel Legourd

R Ce message signifie qu'un programme a démarré automatiquement lors de l'ouverture de la session mais qu'il s'est arrêté aussitôt. Quel est ce programme ? Si le nom du fichier n'est pas significatif, interrogez DOCmémo sur **www.docmemo.com/windows/processus.php**. S'il s'agit d'une application installée sur votre PC, réinstallez-la. Si c'est une application que vous avez désinstallée, bloquez l'exécution automatique de ce fichier au moyen de l'utilitaire de configuration système : cliquez sur *Démarrer*, tapez *msconfig* et enfoncez la touche [Entrée]. Dans la fenêtre de l'utilitaire, passez à l'onglet *Démarrage* et décochez l'élément qui fait référence au fichier indiqué par le message. S'il s'agit d'un spyware (c'est le cas ici), mettez à jour votre antivirus et lancez un scan du disque dur. Essayez aussi avec un antispyware. Par ex. : Ad-Aware (**www.lavasoft.fr**) ou Spybot (**www.safer-networking.org/fr/index.html**). ■

Release by TEAM-DZ

GRAVURE
GRAVEZ UN CD AUDIO

Q ***Je souhaiterais graver des CD audio. J'ai bien Nero, mais installé depuis longtemps, il ne fonctionne pas. Que me conseillez-vous ? Existe-t-il des logiciels gratuits et sérieux ?***

De Paul Deschanel

R Oui, il existe des logiciels de gravure sérieux, gratuits et en français. Par exemple, DeepBurner. Commencez par désinstaller Nero en passant par le module *Ajout/suppression de programmes* ou *Programmes et fonctionnalités* du Panneau de configuration. Téléchargez ensuite DeepBurner Free à partir de la page www.deepburner.com/?r=download. Double-cliquez sur l'icône du fichier téléchargé et laissez faire l'Assistant d'installation en cliquant sur les boutons *Suivant* successifs. Une fois le logiciel installé, double-cliquez sur son icône (elle est sur le Bureau). Le programme est compatible avec toutes les versions de Windows.
Le logiciel vous prend en charge en proposant différents projets et notamment la création d'un CD audio. Cliquez ensuite du bouton droit dans la fenêtre qui s'affiche : le menu qui s'ouvre propose l'ajout de pistes au projet. Sélectionnez les fichiers de musique sur votre disque dur. Quand le disque est complet (voyez les informations dans le coin inférieur gauche), cliquez sur *Graver* dans le volet gauche. ■

IPHONE
LANCEZ LES VIDÉOS FLASH

Q ***Je ne peux pas voir les vidéos sur Dailymotion, pouvez-vous m'aider ?***

De M. Lalique

R Le problème, c'est Flash. Ou plus précisément, c'est Apple qui n'a pas installé de lecteur Flash sur l'iPhone (pas plus que sur l'iPad ou l'iPod). Aucune animation Flash n'est donc visible. C'est gênant car vous ne pouvez pas profiter des vidéos Flash publiées par de nombreux sites, et notamment Dailymotion. Voici comment procéder pour afficher quand même les vidéos Flash. Démarrez Safari et entrez l'adresse www.iosflashvideo.fw.hu. Touchez le bouton du menu puis le bouton *Ajouter un signet*. Validez avec le bouton *Enregistrer*. Touchez ensuite le bouton des signets puis, dans l'écran des signets, le bouton *Modifier*. Sélectionnez *IOSFlashVideo*. Dans le cadre de l'adresse, supprimez tout ce qui précède javascript, c'est-à-dire *www.iosflashvideo.fw.hu/#*. Touchez tous les boutons *Terminer* successifs pour retrouver le navigateur. ■

WINDOWS 7 ET VISTA
RÉACTIVEZ UN SERVICE

Q ***À la suite d'une attaque de virus sur mon OS, plusieurs services Windows ont disparu, dont Windows Update et Windows Installer. Est-il possible de régler ce problème sans réinstaller le système ?***

De René Desvoignes

R Les services n'ont pas vraiment disparu : ils se sont simplement arrêtés et ne démarrent plus automatiquement. Pour réactiver ces services, ouvrez le module *Outils d'administration* du Panneau de configuration et double-cliquez sur *Services*. Dans cette fenêtre, cliquez sur le titre de colonne *Nom* pour afficher les services par ordre alphabétique. Double-cliquez sur *Windows Update*. Dans la liste Type de démarrage, sélectionnez *Automatique*. Cliquez ensuite sur le bouton *Démarrer*. Validez avec *OK* et recommencez la même procédure pour les autres services à réactiver. ■

HOTLINE

MATÉRIEL
PORT USB DÉFICIENT

Q ***Lorsque je connecte mon scanner, j'obtiens le message « Périphérique non reconnu » alors qu'il y a quelque temps, ça fonctionnait correctement. Même chose avec mon imprimante !***

De J. Kanter

R Le problème ne vient pas du pilote des périphériques, mais plutôt celui du port USB. En principe, la réinstallation du pilote USB résout ce genre de tracas. Voici la procédure à suivre : ouvrez le Panneau de configuration et cliquez sur le module *Gestionnaire de périphériques*. Ouvrez la *branche Contrôleur USB générique* et double-cliquez sur *Concentrateur USB générique*. La fenêtre des propriétés s'affiche. Passez à l'onglet *Pilote*. Cliquez sur le bouton *Mettre à jour le pilote*. Dans la fenêtre qui apparaît, cliquez sur *Rechercher un pilote logiciel* sur mon ordinateur. Dans la zone *Emplacement*, entrez *c:\windows\system32*. Cliquez sur *Suivant*, cela réinstalle le pilote.
Répétez l'opération pour les concentrateurs USB mentionnés dans le Gestionnaire de périphériques. Si le problème persiste, désinstallez le concentrateur USB générique (le bouton se trouve dans le Gestionnaire de périphériques) et redémarrez Windows. Il sera automatiquement réinstallé. ■

MESSAGERIE
IMAP EST EN PANNE

Q ***Pour ma messagerie, j'utilise Windows Live Mail. Depuis quelques jours, je ne peux plus consulter mes e-mails. Un message affiche : « Your IMAP server appears to be temporarily out of service ».***

D'Isabelle Sterre

R Les e-mails qui vous sont adressés sont stockés sur un ordinateur. Celui-ci héberge un logiciel qu'on appelle serveur de messagerie. Il existe deux types de serveurs : POP3 et IMAP. Les fournisseurs de messagerie installent toujours un serveur POP3 et proposent de plus en plus souvent un serveur IMAP. Si Windows Live Mail se connecte à un serveur POP3, il récupère les messages en attente. C'est tout ! S'il se connecte à un serveur IMAP, il affiche dans sa fenêtre les dossiers tels qu'ils se présentent sur le serveur, et effectue régulièrement une synchronisation afin de mettre à jour dans sa fenêtre les dossiers et leur contenu. Si le serveur IMAP est en panne, Windows Live Mail ne peut rien afficher. L'alerte que vous voyez signifie que le serveur IMAP est temporairement hors service. Soit vous attendez, soit vous créez un nouveau compte de messagerie connecté cette fois au serveur POP3. Procédez de la manière suivante : cliquez dans le bandeau gauche sur le bouton *Ajouter un compte de messagerie*. Entrez les données d'accès à votre boîte aux lettres sur le serveur POP3 de votre fournisseur. ■

Release by TEAM-DZ

WINDOWS

CD D'ORIGINE ÉGARÉ

Q ***Je dois réinstaller Windows, mais je n'ai pas le CD. Où peut-on se procurer un tel disque?***

De X. Dupléssis

R Lorsque vous faites l'acquisition d'un logiciel ou d'une version de Windows, ce n'est pas le CD, le DVD ou le fichier que vous achetez, mais une licence d'utilisation. Autrement dit, l'important c'est la clé ou le code de licence. Retrouvez ce code. Lancez un appel chez vos amis pour qu'on vous prête un CD ou un DVD de Windows. Si vous avez perdu ce code, il faudra vous procurer un CD ou un DVD avec une licence libre. XP et Vista n'étant plus en vente, voyez les sites de petites annonces ou demandez à vos relations. ■

WINDOWS VISTA ET 7

UNE CLÉ READYBOOST

Q ***Quel type de clé USB puis-je utiliser en mode ReadyBoost sur mon ordinateur équipé de 2 Go de mémoire vive?***

De Stéphane Coltran

R Pour rappel, avec la technologie ReadyBoost, Windows exploite une clé USB ou une carte mémoire Flash comme extension de la mémoire vive, ce qui améliore les performances du système. Pour que Windows active ReadyBoost sur une clé USB, celle-ci doit répondre à quelques caractéristiques techniques précises. Tout d'abord, sa capacité doit être comprise entre 32 Go et 256 Mo avec au minimum 230 Mo d'espace libre. Il faut qu'elle soit au format USB 2.0 et certifiée compatible ReadyBoost, ce qui correspond à un débit de 2,5 Mo/s en lecture et 1,75 Mo/s en écriture. Le temps d'accès moyen doit être inférieur ou égal à 1 ms. Si vous achetez une nouvelle clé, contrôlez si l'emballage indique « ReadyBoost Compatible ». Si vous avez déjà une clé USB, comment savoir si elle est compatible avec ReadyBoost? Facile! Insérez-la dans l'un des ports de votre PC. Si une boîte de dialogue vous invite à activer ReadyBoost, la clé est compatible. Sinon, elle ne l'est pas. Pour activer ReadyBoost sur une clé USB, connectez-la. La fenêtre Exécution automatique s'ouvre. Cliquez sur *Accélérer mon système*. Si cette fenêtre n'apparaît pas, ouvrez l'Explorateur Windows, cliquez du bouton droit sur l'icône de la clé et choisissez la commande *Propriétés*. Passez à l'onglet ReadyBoost. Cochez l'option *Utiliser ce périphérique*. Définissez l'espace à réserver en faisant glisser le curseur jusqu'à la taille recommandée. Si vous utilisez Windows 7, deux choix sont possibles : Dédier ce périphérique à ReadyBoost et Utiliser ce périphérique. Avec la première option, tout l'espace disponible sera réservé à ReadyBoost. Les fichiers déjà présents sur la clé ne seront pas supprimés, mais il sera impossible d'y transférer d'autres fichiers. Avec la seconde, l'espace non occupé par ReadyBoost est disponible pour le stockage de fichiers. Par ailleurs, quelle que soit l'option choisie, la clé reste complètement libre. En d'autres mots, vous pouvez la débrancher et la rebrancher comme vous voulez, sans aucune précaution. ■

WINDOWS 7 ET VISTA

OÙ SONT LES GROS FICHIERS?

Q ***Je voudrais gagner de l'espace sur mon disque dur en déplaçant les fichiers les plus volumineux sur un disque externe. Comment repérer ces fichiers sans devoir regarder le contenu de chaque dossier?***

De Martin Marini

R Ouvrez l'Explorateur Windows. Choisissez la commande *Organiser-Disposition-Volet de recherche*. La barre Recherche avancée s'affiche en haut de la fenêtre. Cliquez sur le bouton fléché situé à son extrémité droite. Dans la liste Emplacement, sélectionnez le lecteur dans lequel vous voulez effectuer la recherche. Déroulez la liste *Taille* et sélectionnez *est supérieur à*. Entrez par exemple la valeur *100 000* pour rechercher les fichiers dont la taille dépasse 100 Mo. Cliquez sur le bouton *Rechercher*. La liste des fichiers trouvés apparaît dans le volet inférieur. Cliquez sur le bouton *Affichage* pour choisir le mode *Détails*. Classez-les par ordre de taille en cliquant sur le titre de la colonne *Taille*. Si cette colonne n'est pas visible, cliquez du bouton droit sur le titre de n'importe quelle colonne et, dans le menu contextuel, cochez *Taille*. Il suffit maintenant de glisser les fichiers vers le disque externe. ■

MATÉRIEL

DISQUES RAID

Q ***Mon ordinateur contient deux disques de 750 Go configurés en Raid 0. Je n'ai eu aucun problème pour créer quatre partitions sur le second disque. Mais il semble impossible de partitionner le premier disque !***

De Thierry Laborde

R Tout d'abord, quelques précisions concernant le Raid 0. Cette configuration regroupe deux disques durs pour qu'ils soient reconnus par le système comme un disque unique. Au moment d'installer Windows, vous avez probablement constaté qu'un seul volume de 1,5 To est disponible. Vous pouvez alors le partitionner normalement au moment de l'installation, ou plus tard avec un logiciel spécialisé (par exemple, Partition Magic). Raid 0 gère les deux disques en parallèle. Pratiquement, des données enregistrées sont réparties automatiquement sur les deux disques physiques, ce qui fournit un espace de 1,5 To. Vous n'avez aucun contrôle sur l'utilisation des disques. Résultat : l'écriture et la lecture des fichiers sont plus rapides. À côté de cet avantage, il y a un gros inconvénient : si un disque dur tombe en panne, toutes les données seront perdues. Les deux disques restent solidaires. Il faut donc prévoir une solution de sauvegarde complémentaire sur un média externe. Il demeure préférable de configurer les disques en Raid 1. Dans ce cas, le second disque s'avère un miroir du premier : le contenu complet du premier disque est copié sur le second. Si le premier disque tombe en panne, le second prend immédiatement le relais, sans aucune perte. Puisque vous avez deux disques de 750 Go, l'espace de stockage utilisable reste limité à 750 Go. Attention, le passage de Raid 0 et Raid 1 entraîne obligatoirement la réinstallation de Windows. Vous pouvez aussi désactiver le Raid et utiliser les deux disques normalement. ■

Release by TEAM-DZ

MESSAGERIE
SPAMS NON FILTRÉS

Q ***J'utilise Windows Live Mail. Pour une raison que j'ignore, les spams (dont l'adresse figure dans la liste des expéditeurs bloqués) ne sont pas dirigés dans la boîte des courriers indésirables.***

De Charles Ferlay

R Le courrier considéré comme du spam est orienté automatiquement vers le dossier Courrier indésirable, à condition que le niveau de détection soit bien réglé. Choisissez la commande *Actions > Courrier indésirable > Options de sécurité*. Passez à l'onglet *Options*. Le niveau Aucun filtrage laisse passer la plupart des spams. Cochez l'un des trois autres niveaux : *Faible*, Élevé ou *Autorisé uniquement*. Attention : le niveau Élevé filtre quasiment la totalité des spams, mais risque de transférer des messages légitimes dans le dossier Courrier indésirable. Contrôlez la liste des expéditeurs bloqués. Celle-ci doit contenir soit des adresses complètes (par exemple : jim@bubble.com), soit des domaines (par exemple : bubble.com). Dans ce cas, tous les e-mails provenant d'un expéditeur @bubble.com seront considérés comme du spam. ■

WINDOWS VISTA ET 7
QUELLE MISE EN VEILLE SÉLECTIONNER ?

Q ***Windows propose trois types de mise en veille : standard, mise en veille prolongée ou mise en veille hybride. Quels sont leurs avantages et leurs inconvénients ? Laquelle choisir ?***

De F. Nicolas

R Avec la mise en veille classique, la mémoire vive reste alimentée et ne perd donc pas son contenu. Si l'alimentation électrique est interrompue, le prochain démarrage sera normal. La veille prolongée stocke le contenu de la mémoire vive sur le disque dur dans le fichier hiberfil.sys. Avec la mise en veille hybride, la mémoire vive reste alimentée et son contenu est transféré sur le disque dur. Au redémarrage, le contenu de la mémoire vive est réactivé et, si celle-ci est vide, c'est le fichier hyberfil.sys qui demeure utilisé. La mise en veille hybride est donc la plus efficace. Pour l'activer, ouvrez le module *Options d'alimentation* du Panneau de configuration. Au niveau du mode de gestion de l'alimentation actif, cliquez sur *Modifier les paramètres du mode* puis sur *Modifier les paramètres d'alimentation avancés*. Dans la rubrique Veille, activez la mise en veille hybride. Dès lors, la commande de mise en veille dans le menu Démarrer correspond à la veille hybride. ■

WINDOWS
UN RÉSIDU COLLANT

Q ***Le message « Windows tente d'ouvrir TrayApp » apparaît à chaque démarrage de Windows. Je ne parviens pas à trouver ce fichier. Je dois chaque fois annuler le message. Comment résoudre ce problème ?***

De Pierre Longchamp

R Ce fichier fantôme est le résidu d'une application mal désinstallée. Il plaçait probablement l'icône du programme dans la zone de notification. Il a été supprimé lors de la désinstallation, mais la commande qui l'exécute au démarrage de Windows n'a pas été effacée. Cliquez sur le bouton *Démarrer* et, dans la zone Rechercher, tapez *msconfig*. Validez avec la touche *Entrée*. Dans la fenêtre Configuration système qui s'ouvre, passez à l'onglet *Démarrage*. Dans la liste, repérez la commande se terminant par trayapp.exe et désactivez-la. Si vous ne la trouvez pas ou si le problème n'est pas résolu, installez CCleaner (www.ccleaner.com/download). Lancez l'application, et dirigez-vous sur le bouton *Registre*. Lancez une recherche d'erreurs, puis une réparation. Acceptez la création d'une sauvegarde des changements. En cas de problème, un double-clic sur l'icône du fichier créé restaurera la Base de registre telle qu'elle était avant la réparation. ■

MULTIMÉDIA
RÉCUPÉREZ UNE BANDE-SON

Q ***Je fais beaucoup de vidéos et je voudrais parfois extraire la bande-son. Comment créer un fichier audio MP3, indépendant de la vidéo dans laquelle il est inclus ?***

De Jean-Pierre Collignan

R Utilisez le logiciel VLC Media Player (**www.videolan.org**). Choisissez la commande *Media-Convertir/Enregistrer*. Dans la boîte de dialogue Ouvrir un média, cliquez sur *Ajouter* et sélectionnez le fichier de la vidéo sur votre disque. Cliquez au bas de la fenêtre sur le bouton *Convertir/Sauvegarder*. La boîte de dialogue Convertir s'ouvre. Cliquez sur *Parcourir* pour choisir le dossier de destination et le nom du futur fichier audio. Attribuez-lui l'extension *mp3*. Cliquez sur *Enregistrer*. Déroulez la liste *Profil* et sélectionnez *Audio-MP3*. Cliquez ensuite, à droite du profil, sur le bouton *Modifier le profil sélectionné*. Cochez la méthode d'encapsulation *WAV*. Passez à l'onglet *Codecs audio*. Cochez l'option *Audio* et sélectionnez le codec *MP3*. Modifiez le débit : entrez la valeur *198 kb/s*. Cliquez sur *Enregistrer* puis sur *Démarrer*. Vous obtenez ainsi un fichier MP3 que vous pouvez écouter et transférer sur un baladeur MP3. ■

Release by TEAM-DZ

HOTLINE

WINDOWS 7
SCANNER BLOQUÉ

Q ***Je viens d'acquérir une machine équipée de Windows 7 64 bits. J'ai réinstallé les programmes utilisés auparavant avec XP sans trop de problèmes, sauf pour mon scanner HP Scanjet 4890. Celui-ci ne fonctionne que partiellement. Et la réinstallation à partir du disque d'origine est refusée par Windows 7 !***

R. Lachenaud

R La version 64 bits de Windows 7 reconnaît certains pilotes 32 bits, mais ceux-ci ne sont pas complètement fonctionnels. Leurs performances restent très réduites. Installez plutôt le pilote 64 bits. Sur la page d'accueil du site d'HP (**http://welcome.hp.com**), cliquez dans la zone de recherche *Support et pilotes* et entrez *scanjet 4890*. La page de l'imprimante s'affiche. Cliquez sur le lien de téléchargement des pilotes. Téléchargez puis installez la version 64 bits pour Windows 7. Il est préférable de désinstaller au préalable le périphérique. Dans le module *Gestionnaire de périphériques*, sélectionnez le scanner et cliquez sur le bouton *Désinstaller*. ■

WORD
UNE MACRO INUTILE

Q ***Lorsque j'ouvre Word 2007, un message intitulé « Microsoft Visual Basic » apparaît m'indiquant une erreur de compilation dans le module caché AZWizardModul. Et rien ne change si je réinstalle Office…***

De Charles Schneider

R Vous avez installé une application qui met en place aussi un module complémentaire dans Word. Ce module est en fait une macro Visual Basic. Mais elle contient des instructions ou des paramètres qui l'empêchent de fonctionner. Word vous informe que la macro est inutilisable. Ce n'est pas grave mais énervant. Supprimez la macro et donc le module afin que ce message n'apparaisse plus. Si vous avez Word 2000, 2002 ou 2003, choisissez la commande *Outils > Macro > Macros*. Sélectionnez *AZWizardModul* et cliquez sur le bouton *Supprimer*. Si vous utilisez Word 2007 ou 2010, cliquez dans l'onglet *Affichage du ruban* sur le bouton *Macros* puis sur *Afficher les macros*. Si Word refuse de supprimer la macro, ouvrez dans le Panneau de configuration *Programmes et fonctionnalités* ou *Ajout/suppression de programmes*. Repérez l'application dont le nom contient AZ et désinstallez-la. ■

WORD 2007 ET 2010
LES IMAGES EN MODE BROUILLON

Q ***Je viens de changer de PC. Sur l'ancien, Word affichait correctement les images en mode* Frappe *ou* Brouillon*. Je ne peux plus les voir qu'en mode* Page*, ce qui est gênant quand on veut appliquer une légende. Comment visualiser les images en mode* Brouillon*?***

De Michel Lagarrigue

R Après avoir inséré une image, sélectionnez-la : Word 2007 ou 2010 complète alors le ruban avec un onglet *Outils > Image > Format*. Activez le mode *Page* Dans celui-ci, cliquez sur *Renvoyer à la ligne automatiquement*. La première option aligne l'image sur le texte. Celle-ci sera donc visible en mode *Brouillon*. Avec les autres options, l'image reste positionnable n'importe où sur la page mais elle n'est visible qu'en mode *Page*. ■

WINDOWS 7
UN DOSSIER VERROUILLÉ

Q ***Dans la fenêtre de l'Explorateur Windows, un cadenas apparaît sur l'icône de certains dossiers. Quand je double-clique dessus, Windows m'interdit de les ouvrir !***

De J.-P. Fernémont

R Ce cadenas signifie que le dossier est verrouillé. Il ne peut être ouvert que par son propriétaire. Il s'agit d'une fonction liée à la sécurité, qui empêche la consultation et la modification déléments non désirées par l'administrateur. Il arrive que Windows prenne l'initiative, sans raison apparente, de verrouiller ainsi certains dossiers en les attribuant à des utilisateurs fantômes. Résultat : puisque vous n'êtes pas le propriétaire, il vous refuse l'accès à ces fichiers alors que vous êtes un utilisateur très réel et possédant des droits d'administrateur. Pour supprimer le cadenas et accéder à vos dossiers, il faut modifier les autorisations de sécurité. Cliquez du bouton droit sur l'icône du dossier et choisissez la commande *Propriétés*. Dans la fenêtre des propriétés, passez à l'onglet *Sécurité*. Cliquez sur le bouton *Modifier* et sélectionnez votre nom d'utilisateur. Cochez *Contrôle total* dans la colonne *Autoriser*. Faites la même chose pour le groupe HomeUsers. Validez avec *OK*. Redémarrez l'ordinateur : le cadenas a disparu et tous les utilisateurs du PC peuvent maintenant ouvrir les dossiers. ■

MATÉRIEL
COUP DE CHALEUR

Q ***Au bout d'environ vingt minutes de fonctionnement, mon PC s'arrête brusquement. La ventilation cesse, l'écran s'éteint, mais sur le boîtier il y a toujours une petite lumière verte clignotante. Pourtant cet ordinateur ne date pas de plus d'un an !***

De Tissiou Vaea

R Votre PC a trop chaud ! Le boîtier contient un capteur thermique qui réagit dès que la température limite est atteinte. Sans cette sécurité, la chaleur provoquerait des dégâts définitifs aux composants de la carte mère, aux barrettes de mémoire vive, au processeur et au disque dur. La plupart des machines sont équipées d'un système de refroidissement adapté à un climat tempéré : un radiateur sur le processeur et un ventilateur sur le boîtier d'alimentation. Commencez par contrôler à l'arrière du boîtier si le ventilateur

tourne, s'il est propre et bien dégagé. Vérifiez également les grilles d'aération. Déplacez le boîtier pour qu'il ne soit pas en plein soleil. Écartez-le du mur afin de laisser l'air circuler. Si ça ne suffit pas, ouvrez le boîtier. Certains processeurs sont recouverts par un radiateur et un ventilateur. Contrôlez si ce ventilateur tourne. S'il est au repos, vérifiez que son câble électrique est bien connecté sur la carte mère. Si ce n'est pas suffisant, ajoutez un ventilateur sur boîtier. ■

Release by TEAM-DZ

WINDOWS

DISQUE INVISIBLE

Q ***Suite à un formatage, mon disque dur externe est introuvable. J'ai essayé de le brancher sur un autre port USB. En vain !***

De Paul Deridder

R Ouvrez le module *Outils d'administration* du Panneau de configuration et double-cliquez sur *Gestion de l'ordinateur*. Dans la fenêtre, cliquez sur *Gestion des disques* dans le dossier *Stockage*. *Repérez le* disque. Cliquez dessus et choisissez la commande *Modifier la lettre de lecteur et le chemin d'accès*. Cliquez sur le bouton *Ajouter* et cochez l'option *Attribuer la lettre de lecteur suivante*. Validez. L'icône du disque est maintenant visible. Si le disque n'apparaît pas, soit il est défectueux, soit le câble USB est endommagé. ■

WINDOWS 7 ET XP

LES POINTS DE RESTAURATION DISPARAISSENT

Q ***J'ai installé Windows 7 en dual boot avec Windows XP. Les points de restauration de Windows 7 disparaissent régulièrement. Comment les conserver ?***

De M. Delagrange

R Ouvrez une session XP. Dans le Poste de travail, notez les lettres des lecteurs pour chacun des OS. Par exemple, C pour Windows XP et E pour Vista ou 7. Lancez *regedit*, l'éditeur de la Base de registre et sélectionnez la clé *HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices*. Choisissez la commande *Édition > Nouveau > Clé*. Nommez la clé *Offline* et sélectionnez-la. Choisissez ensuite *Édition > Nouveau >Valeur DWORD*. Nommez cette valeur *\DosDevices\E:* (puisque le lecteur où est installé Windows 7 porte la lettre E). Double-cliquez sur la valeur et attribuez-lui comme donnée *1*. Fermez *regedit*. Dans le Panneau de configuration, ouvrez le module *Système* et, dans la fenêtre du module, passez sous l'onglet *Restauration du système*. Veillez à ce que le lecteur C (là où est installé XP) soit sous surveillance. Sélectionnez le lecteur *E*. Cliquez sur *Paramètres* et désactivez la restauration du système sur ce lecteur. Fermez la fenêtre du module, et redémarrez le PC sous Windows XP pour que les modifications soient activées. Redémarrez l'ordinateur sous Windows 7. Ouvrez le module *Système* du Panneau de configuration et cliquez dans le volet gauche sur *Protection système*. Vérifiez que la protection est active uniquement sur le volume où Windows 7 est installé. ■

OUTLOOK

UNE RESTRICTION SUSPECTE ET INOPPORTUNE

Q ***Quand je clique sur un lien dans un message, j'obtiens la phrase suivante : « Cette opération a été annulée à cause d'une restriction en vigueur sur cet ordinateur ». Pouvez-vous m'aider à régler ce problème ?***

D'Alain Noiré

R Commencez par quitter Outlook. Ouvrez ensuite *Internet Explorer* et choisissez la commande *Outils > Options Internet*. Dans la boîte de dialogue, cliquez sur l'onglet *Programmes* puis sur le bouton *Utiliser par défaut*. Passez à l'onglet *Avancé* et cliquez sur *Rétablir les paramètres avancés*. Validez. Si le problème n'est pas résolu, lancez *regedit*, l'éditeur de la Base de registre. Sélectionnez la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htmlfile*. Vérifiez si les sous-clés shell, open, command existent. Sinon, créez-les avec la commande *Édition > Nouveau-Clé* de manière à obtenir la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Classes\htmlfile\shell\open\command*. Sélectionnez-la et double-cliquez dans le volet droit sur la valeur (par défaut). Tapez entre guillemets la commande *"C:\Program Files\Internet Explorer\iexplore.exe" %1*. Validez et redémarrez Windows. ■

PHOTO

ISO, ÇA SERT À QUOI ?

Q ***Sur mon appareil photo, je peux régler un paramètre nommé ISO. À quoi sert-il et quand faut-il le modifier ?***

De Thomas Crédent

R Au temps des appareils photos argentiques, on avait le choix entre plusieurs films, en fonction de leur sensibilité à la lumière. Par exemple, un film de 100 ou 200 ISO convenait pour l'extérieur, tandis que dans des conditions de faible éclairage on choisissait un film plus sensible (400 ou 800 ISO…). Pourquoi 800 ISO plutôt que 100 ISO ? Avec un film de 100 ISO, vous devez régler le diaphragme sur 1.4 et la vitesse d'obturation sur 1/30e de seconde. Mais le résultat risque d'être de piètre qualité : pas de profondeur de champ et manque de netteté si vous bougez un peu. En revanche, avec un film de 800 ISO, le diaphragme peut être réglé sur 5.6 et la vitesse d'obturation sur 1/60e de seconde. La qualité des photos sera nettement meilleure. Mais il y a un inconvénient : plus le film est sensible, plus le bruit (ou le grain) sera visible. Le réglage ISO sur un appareil numérique joue le même rôle que pour la photo argentique. ■

Release by TEAM-DZ

ADOBE READER

LOGICIEL INTROUVABLE

Q ***J'ai téléchargé Adobe Reader gratuitement sur un site et à la fin de l'installation, le logiciel était introuvable comme s'il n'était pas installé…***

De Lalloux

R Téléchargez *Adobe Reader* sur le site officiel d'Adobe : http://get.adobe.com/fr/reader. Fermez tous les logiciels ouverts : le navigateur, les applications Office, etc. C'est indispensable pour qu'Adobe Reader puisse procéder à l'installation. Si une application gênante reste ouverte, le logiciel ne sera pas installé. C'est probablement ce qui s'est passé chez vous. Recommencez le téléchargement et l'installation après avoir quitté toutes les applications. ■

SYSTÈME

DE DUAL BOOT À MONO BOOT

Q ***Je possède deux disques durs. Sur l'un Windows XP est installé et sur l'autre Windows 7. Au démarrage du PC, j'ai le choix entre les deux systèmes. Comment enlever complètement XP et le dual boot pour conserver uniquement Windows 7 ?***

De M. Delagrange

R Supposons que Windows XP soit installé sur la partition C et Windows 7 sur la partition D. Commencez par renommer les partitions sur lesquelles sont installés Windows 7 et XP. Dans le menu *Démarrer* de Windows 7, cliquez sur *Ordinateur*. Le système renomme en C la partition sur laquelle il est installé. C'est donc normal que le disque système porte la lettre C, même s'il est effectivement installé sur la partition D. Cliquez du bouton droit sur l'icône du lecteur C et choisissez la commande *Renommer* pour lui attribuer comme nom « Windows 7 ». Un message vous informe que vous devez disposer des droits d'administrateur. Cliquez sur *Continuer*. Attribuez ensuite le nom « Windows XP » à l'icône du lecteur sur lequel XP est installé. Seconde étape : formater la partition « Windows XP ». Insérez le DVD de Windows 7 dans le lecteur et redémarrez le PC sur le DVD. L'Assistant *Installer Windows* se manifeste. Cliquez sur *Suivant* puis sur *Installer maintenant*. Choisissez le type d'installation personnalisée. Les partitions s'affichent. Sélectionnez celle qui se nomme « Windows XP » et cliquez sur *Options de lecteurs* puis sur *Formater*. Une fois la partition formatée, fermez la fenêtre et répondez *Oui* à la question « *Voulez-vous vraiment annuler l'installation de Windows ?* ». Fermez la fenêtre suivante. Troisième étape : réparer le bootmanager. Redémarrez le PC, toujours à partir du DVD. L'Assistant affiche les langues : cliquez sur *Suivant* puis sur *Réparer l'ordinateur*. La fenêtre des options de récupération système s'ouvre. Cochez l'option *Utiliser des outils*. Cliquez sur *Suivant*. La fenêtre propose les outils de récupération. Cliquez sur *Réparation du démarrage* puis sur *Terminer*. Le PC redémarre avec Windows 7. Dernière étape facultative : transférer le disque D sur le disque C. Utilisez un utilitaire de copie et de transfert de l'image d'une partition. Par exemple : Macrium Reflect. Ce logiciel est gratuit. Téléchargez-le ici : www.macrium.com/reflectfree.asp. ■

MATÉRIEL

TOUCHE [F1] OBLIGATOIRE ?

Q ***Depuis quelques jours, je dois presser la touche [F1] pour que mon PC démarre. L'écran affiche le message suivant :*** **« Master Hard Disk : S.M.A.R.T. Status BAD, Backup and Replace »**. ***Comment faire pour que mon ordinateur démarre normalement ?***

De Jean-Yves Le Sann

R Ce message est dû à la sollicitude d'un système nommé S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology). Cette technologie, utilisée par certains disques durs, part du principe qu'un disque ne tombe pas brusquement en panne, mais se dégrade petit à petit. Elle prévient les accidents futurs en fonction de plusieurs critères fondés sur l'utilisation du disque. Il ne s'agit donc pas d'un constat résultant de la détection d'un problème réel, mais d'une estimation statistique. Ce système n'est pas tout à fait au point. En fait, le disque peut tomber en panne demain ou dans cinq ans, ce qui n'est pas une info très utile ! Vous avez donc le choix entre le remplacement du disque et la désactivation de S.M.A.R.T. dans le programme de configuration du Bios. Pour y accéder, pressez la touche qui donne accès au Setup. Cherchez une option dont l'intitulé contient le mot SMART et attribuez-lui la valeur *Disabled* (désactivé). ■

WINDOWS 7 OU VISTA

READYBOOST NE RÉPOND PAS

Q ***J'ai activé ReadyBoost sur une clé USB de 4 Go mais elle ne fonctionne que quelques minutes… Ensuite, plus rien !***

De Claude Bernard

R Pour rappel, avec la technologie ReadyBoost, Windows (32 ou 64 bits) exploite une clé USB comme extension de la mémoire vive. Pour que Windows active ReadyBoost sur une clé, sa capacité doit être comprise entre 32 Go et 256 Mo, avec au minimum 230 Mo d'espace libre. Il faut qu'elle soit au format USB 2 et enfin, elle doit avoir à un débit de 2,5 Mo/s en lecture et 1,75 Mo/s en écriture. Le temps d'accès moyen doit être inférieur ou égal à 1 ms. Si vous achetez une nouvelle clé USB, contrôlez si l'emballage indique « ReadyBoost Compatible ». Pour activer ReadyBoost sur une clé, connectez-la. La fenêtre *Exécution automatique* s'ouvre. Cliquez sur le bouton *Accélérer mon système*. Si cette fenêtre n'apparaît pas, ouvrez l'*Explorateur Windows*, cliquez du bouton droit sur l'icône de la clé et choisissez la commande *Propriétés*. Passez à l'onglet *ReadyBoost*. Cochez l'option *Utiliser ce périphérique*. Définissez l'espace à réserver en faisant glisser le curseur jusqu'à la taille recommandée. Si vous utilisez Windows 7, deux choix sont possibles : *Dédier ce périphérique à ReadyBoost* et *Utiliser ce périphérique*. Avec la première option, tout l'espace disponible sera réservé à ReadyBoost. Les fichiers déjà présents sur la clé ne seront pas supprimés, mais il sera impossible d'y transférer d'autres fichiers. Avec la seconde, l'espace non occupé par ReadyBoost est disponible pour le stockage de fichiers. Par ailleurs, quelle que soit l'option choisie, la clé USB reste complètement libre. En d'autres termes, vous pouvez la débrancher et la rebrancher comme vous voulez, sans aucune précaution. ■

Release by TEAM-DZ

WINDOWS
AUTOMATISEZ L'OUVERTURE DE LA SESSION

Q ***J'ai lu quelque part qu'il est possible de démarrer Windows et d'ouvrir une session sans devoir entrer son mot de passe. Pouvez-vous me rappeler la procédure ?***

De Bernard Mura

R Cliquez sur *Démarrer* et tapez *control userpasswords2*. Tous les comptes installés sont affichés. Dans l'onglet *Utilisateurs*, vous pouvez annuler l'obligation de montrer patte blanche : désactivez l'option *Les utilisateurs doivent entrer un nom d'utilisateur et un mot de passe*. Cliquez sur *Appliquer* et entrez le nom et le mot de passe de la session qui s'ouvrira automatiquement au démarrage de Windows. À l'inverse, l'onglet *Options avancées* permet notamment de sécuriser l'ouverture des sessions en obligeant à appuyer sur la combinaison de touches [Ctrl] + [Alt] + [Suppr] pour entrer le nom et le mot de passe. Cette procédure fonctionne avec les versions professionnelles de Windows. Sinon, il faut passer par la Base de registre. Sélectionnez la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon*. Créez si nécessaire les trois valeurs chaînes : *DefaultUserName*, *DefaultPassword*, *AutoAdminLogon*. Entrez pour ces valeurs les données suivantes : le nom d'utilisateur (*DefaultUserName*), le mot de passe (*DefaultPassword*), 1 (*AutoAdminLogon*). Si vous souhaitez ponctuellement ouvrir une session avec un autre compte, appuyez sur la touche [Maj] pendant le processus de démarrage. ■

WINDOWS
MAJ IMPOSSIBLES

Q ***Depuis quelque temps, il est impossible de faire les MAJ. Quand je clique sur Windows Update, j'obtiens le message suivant : « Windows Update ne peut pas actuellement rechercher des mises à jour car le service n'est pas en cours d'exécution »...***

De Léon Allaire

R Un service est un module de l'OS qui fonctionne en arrière-plan. Certains services démarrent automatiquement avec Windows : ils sont ainsi prêts à fonctionner dès que Windows ou une application en a besoin. Windows Update est un service qui, normalement, démarre à l'ouverture de Windows. Chez vous, pour le réactiver, ouvrez le module *Outils d'administration* du Panneau de configuration et double-cliquez sur *Services*. Dans la fenêtre, cliquez sur le titre de colonne *Nom* pour afficher les services par ordre alphabétique. Double-cliquez sur *Windows Update*. Dans la liste *Type de démarrage*, sélectionnez *Automatique*. Cliquez ensuite sur le bouton *Démarrer*. Validez avec *OK*. ■

INTERNET EXPLORER
GOOGLE EN FRANÇAIS

Q ***Internet Explorer permet le choix du moteur de recherche de façon permanente. J'ai choisi Google. Internet Explorer me connecte à Google.com et non à Google.fr. Inconvénient : si les mots de la requête contiennent un tant soit peu d'anglais, ce sont les sites en anglais qui sont affichés en premier.***

De François Legrand

R Si vous lancez une recherche avec des mots-clés en anglais, les résultats correspondent à des sites en anglais. C'est normal, quel que soit le site de Google (google.com ou google.fr). En revanche, lorsque vous ajoutez Google dans la liste des moteurs de recherche d'Internet Explorer, c'est la version américaine du moteur qui est activée et donc, les commandes et les options sont en anglais. Pour modifier l'adresse de Google afin de remplacer google.com par google.fr, démarrez *regedit*, l'éditeur de la Base de registre et sélectionnez la clé *HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchScopes*. Sélectionnez une à une les sous-clés pour repérer celle qui correspond à Google (voyez dans le volet droit le contenu de la valeur *DisplayName*). Double-cliquez alors sur la valeur URL et remplacez *www.google.com* par *www.google.fr*. ■

INTERNET EXPLORER
DOSSIER PAR DÉFAUT

Q ***Comment définir le dossier par défaut pour le téléchargement des fichiers à partir d'Internet Explorer ?***

De Michel Reboul-Millet

R Ouvrez *regedit*, l'éditeur de la Base de registre. Sélectionnez la clé *HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer* et double-cliquez sur la valeur *Download Directory*. Elle contient le chemin complet du dossier qui sera proposé lors du prochain téléchargement. Remplacez-la par le chemin d'un dossier de votre choix. Lors du prochain téléchargement, c'est donc ce dossier qui sera suggéré. Vous aurez le droit de le modifier et, dans ce cas, c'est ce nouveau dossier qui sera enregistré dans la Base de registre et donc proposé la prochaine fois. Pour empêcher toute modification de la valeur *Download Directory*, sélectionnez-la et choisissez la commande *Édition-Autorisations*. Cliquez sur le bouton *Avancé*. Sélectionnez votre nom d'utilisateur dans la liste et cliquez sur le bouton *Modifier*. Repérez l'autorisation *Définir la valeur* et cochez la case de la colonne *Refuser*. Validez en cliquant sur *OK*. ■

Release by TEAM-DZ

HOTLINE

WINDOWS
SOFT À DÉSINSTALLER

Q ***J'ai désinstallé une ancienne version de Norton Internet Security en passant par le module* Programmes et fonctionnalités *du Panneau de configuration, mais la désinstallation est incomplète. Il reste des éléments à démarrage automatique. Comment me débarrasser complètement de Norton Internet Security ?***

De R. Lassine

R Utilisez l'utilitaire fourni par Symantec, l'éditeur des logiciels Norton. Téléchargez-le ici : **ftp://ftp.symantec.com/public/english_us_canada/removal_tools/Norton_Removal_Tool.exe**. Double-cliquez ensuite sur l'icône du fichier et suivez les instructions à l'écran. Vous devrez peut-être redémarrer plusieurs fois Windows ou répéter à maintes reprises la même opération. N'ayez aucune crainte, c'est tout à fait normal. Suivez à la lettre les instructions. Cet utilitaire de désinstallation convient aux versions 2003, 2004, 2005, 2006 et 2007 de tous les logiciels Norton et elle règlera votre problème de programme résiduel et de ralentissement. ■

INTERNET
FLASH EN 64 BITS

Q ***Sur mon PC Windows 7 64 bits, Internet Explorer 8 ne cesse de me demander l'installation du module complémentaire Adobe Flash Player.***

De M. Pereira

R Actuellement, le lecteur Flash compatible avec la version 64 bits d'Internet Explorer est encore en version bêta, sous le nom de Flash Player Square. Vous pouvez l'installer mais vous rencontrerez peut-être des problèmes. Téléchargez-le ici : http://labs.adobe.com/downloads/flashplayer10_square.html. Cliquez sur le lien *Download active-x for 64-bit Windows – for Internet Explorer only*. Une version différente (plug-in for 64-bit Windows – for all other browsers) est prévue pour les autres navigateurs (Firefox, Opera, Safari, etc.). En attendant la version définitive de Flash Player Square, utilisez plutôt la version 32 bits d'IE : vous trouverez son fichier exécutable sur votre disque dur dans le dossier *C:\program Files (x86)\Internet Explorer*. Double-cliquez sur l'icône *iexplore*. Passez ensuite par le module *Programmes et fonctionnalités* du Panneau de configuration pour désinstaller une éventuelle ancienne version de Flash Player. Installez ensuite la version 32 bits à partir de la page http://get.adobe.com/fr/flashplayer. ■

MESSAGERIE
ARNAQUE OU NON?

Q ***Je reçois de temps en temps un e-mail qu'on me demande de faire suivre ; le dernier était une demande d'aide pour une opération chirurgicale. Comment savoir s'il s'agit d'un message sérieux ?***

De G. Jourdan

R Interrogez le site Hoaxkiller (www.hoaxkiller.fr). Si vous choisissez la recherche par mots clés, entrez des noms significatifs contenus dans le message. Par exemple : un numéro de téléphone, un mot représentant le thème du message… Entrez les mots tels qu'ils sont orthographiés et séparez-les par un espace. Si vous préférez une recherche par texte intégral, collez dans le formulaire le texte complet du message reçu. Cochez l'option *Rechercher par texte intégral* avant de cliquer sur le bouton *Recherche Hoaxkiller.fr*. ■

INTERNET
UN NOUVEL ONGLET POUR CHAQUE LIEN

Q ***Habituellement, lorsque j'ouvre un lien vers une page internet à partir d'Excel, la page web s'affiche dans un nouvel onglet de la fenêtre d'Internet Explorer en cours. Depuis peu, cette ouverture se fait dans une nouvelle fenêtre d'IE. Donc autant de liens cliqués, autant de fenêtres ouvertes. C'est très encombrant et pas toujours facile à gérer.***

De Daniel Falandry

R Dans la fenêtre d'Internet Explorer, choisissez la commande *Outils > Options Internet*. Dans l'onglet *Général*, cliquez sur le bouton *Paramètres* de la section *Onglets*. Cochez l'option *Ouvrir les liens des autres programmes dans un nouvel onglet de la fenêtre active*. Passez ensuite à l'onglet *Avancé* et décochez l'option *Réutiliser les fenêtres pour lancer des raccourcis*. Redémarrez *Internet Explorer*. Si le problème n'est pas résolu, ouvrez à nouveau les options internet. Dans l'onglet *Avancé*, cliquez sur le bouton *Réinitialiser*. Les liens s'ouvrent toujours dans une nouvelle fenêtre ? Lancez *regedit*, l'éditeur de la Base de registre. Sélectionnez la clé *HKEY_CLASSES_ROOT\Interface\{79EAC9C5-BAF9-11CE-8C82-00AA004 BA90B}*. La valeur (par défaut) doit avoir pour donnée IHlinkFrame. ■

EXCEL
UN CLASSEUR PERDU

Q ***Je ne parviens plus à ouvrir un fichier Excel en double-cliquant sur son icône, ni même en passant par la commande* Fichier > Ouvrir. *Est-il définitivement perdu ?***

De Jean Rouge

R Commencez par ouvrir un document vide dans Word. Dans l'onglet *Insertion du ruban*, cliquez sur le bouton *Insérer un objet*. Dans l'onglet *Créer à partir du fichier*, cliquez sur le bouton *Parcourir* pour sélectionner le fichier Excel. Essayez également ceci : créez un classeur vide et enregistrez-le dans le même dossier que celui qui pose problème. Dans la cellule A1 de la première feuille de calcul, entrez la formule suivante : *='[classeur endommagé.xls]nom feuille'!A1*. Remplacez bien sûr *classeur endommagé* par le nom de votre classeur, et nom feuille par le nom de sa première feuille. Copiez cette formule vers le bas et vers la droite. Sélectionnez toute la feuille (en cliquant sur la case vide située dans le coin supérieur gauche de la feuille) et copiez-la dans le presse-papiers en appuyant sur les touches [Ctrl] + [C]. Choisissez la commande *Édition > Collage spécial*. Dans la boîte de dialogue qui s'affiche, cochez *Valeurs* et validez. Les formules sont ainsi remplacées par leur valeur, ce qui supprime tout lien avec le classeur défectueux. Répétez cette procédure pour chaque feuille du classeur. Avec ces deux méthodes, vous récupérez uniquement les valeurs : les formules, les formats, les macros sont définitivement perdus. ■

Release by TEAM-DZ

GRAVURE

100 % DE RÉUSSITE

Q ***Je grave souvent des CD audio avec le lecteur Windows Media. Parfois, la gravure échoue. J'ai essayé de changer de marque de CD mais rien n'y fait!***

De Thomas Gallois

R Le lecteur Windows Media est configuré pour graver à la vitesse maximale supportée par le périphérique. Mais cela reste souvent trop rapide pour éviter les erreurs, surtout si vous continuez à utiliser le PC pendant la gravure. Il est donc préférable de réduire cette vitesse. Cliquez sur la petite flèche située sous le bouton *Graver*. Dans le menu qui s'ouvre, choisissez la commande *Options supplémentaires*. Dans la boîte de dialogue *Options* qui s'affiche, ouvrez la liste *Vitesse de gravure* et sélectionnez *Moyenne*. Si les problèmes persistent, essayez avec un autre graveur. ■

OUTLOOK

LE TRANSFERT D'E-MAILS D'UN ORDINATEUR À UN AUTRE

Q ***Je voudrais transférer le courrier reçu sur mon PC portable pendant un déplacement vers mon ordinateur lorsque je rentre au bureau.***

D'Alain Noire

R Outlook stocke toutes les données dans un unique fichier. Sauvegardez ces infos en vrac ou en extrayant uniquement ce qui vous intéresse. Objectif : faire des copies de sécurité de vos données pour ensuite les restaurer ou les transférer sur un autre ordinateur. Votre dossier personnel est enregistré sur le disque dur dans un fichier portant l'extension pst. Lorsque vous archivez, sauvegardez ou exportez des données, Outlook génère des fichiers pst. Il peut ouvrir et donc vous donner accès simultanément au contenu de plusieurs fichiers pst. Choisissez la commande *Fichier > Importer et exporter*. Avec Outlook 2010, cliquez sur l'onglet *Fichier* puis sur *Options* et enfin, dans la catégorie Options avancées, sur le bouton *Exporter*. L'Assistant d'importation et d'exportation démarre. Sélectionnez l'action *Exporter des données vers un fichier* puis le type de fichier *Fichier de données Outlook*. Choisissez ensuite *Dossiers personnels* et cochez l'option *Inclure les sous-dossiers*. Cliquez sur le bouton *Suivant* puis sur *Parcourir* pour sélectionner la destination du fichier qui sera créé. Indiquez le nom du fichier en lui donnant l'extension *.pst*. Cliquez sur le bouton *Terminer*. Le fichier est créé et apparaît en tant que dossier personnel dans la fenêtre d'Outlook. Fermez-le en cliquant du bouton droit sur son nom et en choisissant la commande *Fermer*. Pour ouvrir le fichier de sauvegarde, choisissez la commande *Fichier > Ouvrir > Fichier de données Outlook* ou, avec Outlook 2010, cliquez sur l'onglet *Fichier* puis sur *Ouvrir* et enfin sur *Ouvrir le fichier de données Outlook*. Sélectionnez le fichier pst à ouvrir. Outlook affiche son contenu dans un dossier portant le nom du fichier. Pour récupérer un élément (par exemple un e-mail), sélectionnez-le dans le dossier de sauvegarde et glissez-le dans un sous-dossier de votre dossier personnel. Terminez l'opération en fermant le dossier de la sauvegarde : cliquez du bouton droit sur son nom et choisissez la commande *Fermer*. ■

INTERNET

CLIQUEZ SUR LES LIENS

Q ***Comment ouvrir un lien dans un e-mail reçu ? J'utilise Internet Explorer 9 et Windows Live Mail 2011.***

De Robert Thomas

R Normalement, il suffit de cliquer sur un lien pour que le navigateur s'active et affiche la page correspondant à cette adresse. Première chose à contrôler : est-ce qu'Internet Explorer est bien le navigateur par défaut ? Pour le savoir, choisissez dans la fenêtre d'IE la commande *Outils > Options Internet*. Dans l'onglet *Programmes*, cliquez sur le bouton *Utiliser par défaut*. Si le problème n'est pas résolu, ouvrez la fenêtre d'invite de commande, tapez *RegSvr32 urlmon.dll* et validez avec la touche [Entrée]. Si la difficulté persiste, tapez une à une les commandes suivantes en les validant chaque fois avec [Entrée] : *RegSvr32 Mshtml.dll*, *RegSvr32 Actxprxy.dll*, *RegSvr32 Oleaut32.dll*, *RegSvr32 Shell32.dll*, *RegSvr32 Shdocvw.dll*, *RegSvr32 Msjava.dll*, *RegSvr32 Browseui.dll*. Si les liens ne sont toujours pas fonctionnels, ouvrez *Internet Explorer* et choisissez la commande *Outils > Options*. Dans l'onglet *Avancé*, cliquez sur le bouton *Réinitialiser* et confirmer la remise à zéro d'Internet Explorer. Validez puis redémarrez Windows. ■

MESSAGERIE

DES ADRESSES OBSOLÈTES

Q ***Dans la fenêtre de création d'un message, lorsque je commence à taper l'adresse du destinataire, une liste s'ouvre. Elle contient des adresses erronées ou qui ne sont plus valables. Comment nettoyer cette liste ?***

De Michel Porti

R Ce système de saisie semi-automatique fonctionne dans les champs A, Cc et Cci. La liste proposant des adresses est complètement indépendante du carnet d'adresses. Elle contient les 29 dernières adresses entrées précédemment. La désactivation (et l'activation) de cette fonction dépend d'une option qui diffère en fonction de la version d'Outlook. Si vous utilisez Outlook Express ou Windows Live Mail, choisissez la commande *Outils > Options* et passez sous l'onglet *Envois*. Décochez l'option *Compléter automatiquement l'adresse de messagerie lors de la saisie*. Si vous utilisez Outlook 2002, 2003 ou 2007, choisissez la commande *Outils > Options*. Dans l'onglet *Préférences* de la fenêtre des options, cliquez sur *Options de la messagerie*. Dans la nouvelle fenêtre, cliquez sur le bouton *Options avancées de la messagerie*. Décochez *Suggérer les noms lors de la saisie des champs A, Cc et Cci*. Si vous utilisez Outlook 2010, cliquez sur l'onglet *Fichier* puis sur *Options*. Dans la catégorie *Courrier*, cochez l'option *Utiliser la liste de saisie automatique*. Le bouton *Vider la liste de saisie semi-automatique* supprime toutes les suggestions en cours. Pour effacer un seul élément de cette liste, commencez à entrer l'adresse. Quand la liste apparaît, sélectionnez avec les flèches du clavier l'adresse que vous voulez supprimer et appuyez sur la touche [Suppr]. Cette suppression ne se répercute pas dans le carnet d'adresses : seule la liste de saisie semi-automatique est affectée. ■

Release by TEAM-DZ

OUTIL DE GESTION

ACCÈS REFUSÉ

Q ***Je suis administrateur sur mon PC portable et, pourtant, je ne peux pas ouvrir la console gpedit.msc. Lorsque je tape le nom de ce fichier dans le menu* Démarrer*, il ne se passe rien !***

De Pierre Dollé

R Ce fichier correspond à la console de l'éditeur de stratégie de groupe locale. Cette console demeure absente de Windows Premium (XP, Vista ou Windows 7). Si vous utilisez Windows XP, vous pouvez l'installer manuellement. Commencez par télécharger le fichier www.astwinds.com/Logiciels/gepeditxphome/gpedit%20pour%20xp%20home.zip et décompressez-le. Ouvrez enfin le dossier contenant les fichiers décompressés et double-cliquez sur *gpedInst.bat*. Le programme d'installation copie les fichiers DLL nécessaires dans le dossier c:\Windows\System32 ou c:\Windows\System32\GroupPolicy\Adm et les active. Ensuite, la commande *gpedit.msc* démarre la console. ■

INTERNET

INTERNET EXPLORER, PLUS LENT QU'UN ESCARGOT

Q ***Depuis quelque temps, le surf avec Internet Explorer est devenu très lent. Comment retrouver la vitesse d'origine ?***

De M. Obapo

R Lorsqu'Internet Explorer s'ouvre, il charge en mémoire plusieurs modules complémentaires. Le navigateur n'est pas disponible tant que tous les modules actifs ne sont pas chargés. Par ailleurs, certains modules vont être chargés quand ils sont nécessaires, pendant que vous surfez. Un module trop long à charger peut donc ralentir le démarrage d'IE ou freiner la navigation. Choisissez la commande *Outils > Gérer les modules complémentaires*. La fenêtre de gestion des modules complémentaires s'ouvre. Dans la liste, sélectionnez *Tous les modules complémentaires*. Dans le volet droit, glissez le bouton de défilement à l'extrême droite afin de visualiser la colonne *Durée de chargement*. Cliquez sur le titre de la colonne pour classer les modules en fonction de cette durée. Si vous repérez un module trop lent, sélectionnez-le et mettez-le hors service en cliquant sur le bouton *Désactiver*. Si vous ne pouvez pas désactiver un module gênant, démarrez le navigateur en mode allégé, c'est-à-dire sans charger aucun module. Cliquez sur le bouton *Démarrer* de Windows. Avec Vista ou Windows 7, cliquez dans la zone *Rechercher*. Avec XP, cliquez sur *Exécuter*. Dans tous les cas, tapez la commande *iexplore > extoff* et pressez la touche [Entrée]. Passez par le menu *Outils* pour accéder à la fenêtre de gestion des modules complémentaires et désactivez le module gênant. Voyez également s'il est possible de la désinstaller dans le module *Programmes et fonctionnalités* du Panneau de configuration. ■

CLÉ USB

UNE CLÉ EN SOUS-CAPACITÉ

Q ***Ma clé USB avait à l'origine une capacité de 4 Go. Je viens de constater qu'elle ne dispose plus que de 3,6 Go d'espace de stockage. Comment récupérer tout l'espace de cette clé ?***

De Matthieu Poltier

R En général, il s'agit d'un problème de système de fichiers inadéquat ou endommagé. Lisez le manuel de la clé pour vérifier s'il existe un utilitaire de formatage ou de réinitialisation. Si vous ne trouvez aucune consigne spécifique, essayez une procédure générale. Dans le Panneau de configuration, ouvrez le module des outils d'administration. Double-cliquez sur l'icône *Gestion de l'ordinateur*. Dans la fenêtre qui s'ouvre, ouvrez le dossier *Stockage* puis cliquez sur *Gestion des disques*. Si la clé contient plusieurs partitions, supprimez-les. Cliquez du bouton droit sur une partition et choisissez la commande *Supprimer la partition*. Formatez ensuite la clé en FAT32. Cliquez du bouton droit sur le nom de la clé et choisissez la commande *Formater*. Notez qu'une différence d'environ 10 % est parfois normale. Elle est due à l'évaluation du Mo par le fabricant : 1 million d'octets ou 1 048 576 octets (1 024 x 1 024). Une clé de 4 Go peut donc afficher 4 millions ou 4 194 304 octets. ■

MATÉRIEL

QUEL TYPE DE DVD CHOISIR ?

Q ***Quelle est la différence entre un DVD+RW et un DVD-RW ?***

De Christian Desolare

R Il faut savoir que les deux lettres RW signifient « Rewritable » (réinscriptible). On peut graver, effacer et regraver ce type de DVD jusqu'à 1 000 fois. En revanche, les DVD-R et +R ne peuvent être gravés qu'une seule fois. Il est impossible de les effacer. Actuellement, on trouve deux normes de DVD réinscriptibles. En pratique, le résultat est identique, quelle que soit la norme. Il faut plutôt contrôler le type de DVD que votre graveur accepte. Normalement, les graveurs récents sont multistandards : ils s'adaptent aux DVD+R, +RW, -R et -RW. Si les DVD que vous gravez sont destinés à être lus sur un PC, les deux normes se valent. Si les DVD doivent être lus sur différents types de matériel, choisissez de préférence les DVD-R : ils sont reconnus par tous les lecteurs, même les plus anciens modèles. En revanche, les DVD+R ne restent lisibles que par les appareils récents. Si votre lecteur refuse l'un ou l'autre standard, essayez de mettre à jour son firmware (le logiciel interne qui contrôle le fonctionnement du graveur). Voyez ce que propose le constructeur sur son site. ■

Release by TEAM-DZ

WINDOWS 7
WMC : LANCEMENT AUTOMATIQUE

Q ***Je dispose de Windows 7 et Vista en dual boot sur mon PC. Un menu de démarrage me permet donc de choisir le système. Je désirerais ajouter une option pour lancer directement le logiciel Windows Media Center (en version Windows 7) depuis ce menu de démarrage. Est-ce possible ?***

De Claude Replessis

R Ce menu sert exclusivement à proposer les systèmes d'exploitation et à mettre en service celui qui est choisi. Il est impossible, par son intermédiaire, de lancer une application. La seule solution consiste à glisser dans le dossier *Démarrage* du menu *Démarrer* une copie du raccourci de l'application. Faites comme ceci : dans le menu *Démarrer*, cliquez du bouton droit sur la commande qui lance l'application et glissez son icône sur le dossier *Démarrage*. Patientez deux secondes : quand le dossier s'ouvre, glissez l'icône dans la liste des raccourcis qui y sont déjà. Dans le cas de Windows Media Center, c'est encore plus simple. Ouvrez-le et sélectionnez *Tâches* puis *Paramètres*. Cliquez sur *Général* puis sur *Démarrage et comportement de la fenêtre*. Cochez l'option *Démarrer Windows Media Center en même temps que Windows*. Validez en cliquant sur *Enregistrer*. ■

MATÉRIEL
LE PROCESSEUR SUR LE POINT DE GRILLER

Q ***Chaque fois que mon PC démarre, il se bloque sur le message « CPU fan error – Press F1 to resume ». Je presse la touche [F1] et le démarrage se poursuit alors normalement.***

De Paulette Testas

R Ce message vous informe que le ventilateur du processeur est en panne. Le processeur est l'un des composants qui chauffe le plus. Il est refroidi par un ventirad (c'est-à-dire la combinaison d'un ventilateur et d'un radiateur). Si celui-ci ne fonctionne plus, le processeur risque de se détériorer par excès de chaleur. Éteignez l'ordinateur et déconnectez sa prise électrique. Ouvrez son capot et contrôlez si le ventirad est correctement positionné.
Contrôlez également si le fil par lequel il s'alimente en électricité est bien branché sur le connecteur de la carte mère. S'il est en panne, remplacez-le. Achetez un modèle similaire, compatible avec le processeur. Pour faciliter cet achat, déclipsez-le et montrez-le au vendeur. Ne tardez pas car, sans refroidissement, le processeur risque vraiment de griller. ■

WINDOWS
OÙ SONT LES DOUBLONS ?

Q ***Je suis à la recherche d'un logiciel capable de retrouver les doublons dans les fichiers stockés sur mon disque dur.***

De Michel Joubert

R Duplicate Cleaner (www.digitalvolcano.co.uk/content/duplicate-cleaner - gratuit et en français) repère et efface les fichiers en double. Pour les détecter, il se base sur le nom des fichiers mais aussi les tailles et les dates. Pour les fichiers musicaux, il recherche également dans les métadonnées (le nom de l'artiste, le titre, l'album). Les doublons sont regroupés dans l'onglet *Fichiers dupliqués*. Avant de les supprimer, contrôlez leur contenu au moyen de la visionneuse intégrée. Vous pouvez aussi sauvegarder la liste dans un fichier texte afin d'effectuer le contrôle manuellement. ■

MATÉRIEL
LE LECTEUR DE DVD RESTE INVISIBLE

Q ***Depuis quelques jours, mon lecteur de DVD n'est plus reconnu. Il n'apparaît plus dans le Gestionnaire de périphériques.***

De Christophe Lebec

R Microsoft propose une application de résolution de problèmes divers : Fix It Center. Téléchargez-la à partir du site d'aide de Microsoft à l'adresse http://fixitcenter.support.microsoft.com/Portal. Cliquez sur le bouton *Essayez dès maintenant* puis, dans la fenêtre de téléchargement, sur *Exécuter*. Lors de l'installation, acceptez le paramétrage immédiat de l'application. Le programme cherche alors les modules de résolution de problèmes adaptés à votre ordinateur et à vos périphériques. Parmi ceux-ci, un module est consacré aux périphériques matériels non détectés. Vous n'êtes pas obligé d'installer tous les modules. Décochez ceux qui ne vous intéressent pas : vous pourrez les installer plus tard s'ils s'avèrent nécessaires. Cliquez sur *Suivant*. Dans la fenêtre de Microsoft Fix Center, dirigez-vous sur le bouton *Exécuter* correspondant à l'utilitaire *Périphériques matériels non détectés* et suivez les instructions. Par la suite, vous retrouverez Microsoft Fix Center dans le menu *Démarrer*. Plutôt que de télécharger l'application, cherchez une solution en ligne : sur le site Fixit Center Online, cliquez sur *Trouver des solutions*. Sélectionnez alors votre version de Windows puis la catégorie du problème. Dans votre cas, *Matériel et pilotes*. Explorez ensuite les suggestions proposées par Microsoft. ■

HOTLINE

INTERNET EXPLORER
UNE VALEUR ABSENTE

Q ***Dans le numéro de mars, j'ai lu avec attention la réponse concernant le dossier de téléchargement par défaut des fichiers à partir d'Internet Explorer. Vous conseillez de modifier la valeur* Download Directory, *située au niveau de la clé* HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer. *Cette valeur n'existe pas sur mon PC. Comment faire alors ?***

De Michel Reboul-Millet

R En général, quand une valeur est absente de la Base de registre, c'est sa donnée par défaut qui est active. Pour modifier la donnée par défaut, il faut alors créer la valeur. Sélectionnez la clé dans laquelle la valeur doit se trouver. Dans notre exemple : *HKEY_CURRENT_USER\Software\ Microsoft\Internet Explorer*. Passez par la commande *Edition > Nouveau* et cliquez sur le type de valeur à créer. Dans notre cas : *Valeur chaîne*. La nouvelle valeur est tout de suite insérée dans le volet gauche sous le nom *Nouvelle valeur #1*. Renommez-la. Par exemple : Download Directory. Respectez scrupuleusement l'espace. Double-cliquez ensuite sur la valeur pour introduire sa donnée. ■

Release by TEAM-DZ

OFFICE 2007 ET 2010

DES MODULES CACHÉS

Q ***À l'ouverture d'Excel 2007, j'obtiens le message suivant : « Microsoft Visual Basic - Erreur de compilation dans le module caché : AutoExecNew ». Et à la fermeture : « Microsoft Visual Basic - Erreur de compilation dans le module caché : DistMon ».***

De Robert Cuidard

R Le dossier Office Startup (*C:\ProgramFiles\MicrosoftOffice\Office(numéro)\STARTUP*) ou le dossier Excel Startup (*C:\ProgramFiles\Microsoft Office\Office (numéro)\XLSTART*) contient des fichiers qui s'ouvrent automatiquement au démarrage d'une application Office ou d'Excel. Ouvrez ces dossiers et supprimez les fichiers qu'ils contiennent. Ils sont en rapport avec Adobe Reader, le logiciel de lecture des fichiers PDF. Réinstallez ensuite Acrobat Reader en le téléchargeant ici : http://get.adobe.com/fr/reader. ■

WINDOWS XP ET 7

LE RÉSEAU LOCAL NE FONCTIONNE PAS BIEN

Q ***Les trois ordinateurs de ma maison (Windows 7 et Windows XP) sont connectés par un câble ou par Wi-Fi à ma box internet. Sur chaque ordinateur, quelques dossiers sont partagés. Malgré tous mes efforts, les ordinateurs ne se « voient » pas.***

D'Alex

R Chaque ordinateur du réseau local est identifié par une adresse IP. Cette adresse, composée de quatre nombres compris entre 0 et 256, doit absolument être différente pour chaque. Par exemple, 192.168.0.12, 192.168.0.13, … Pour attribuer cette adresse, vous avez le choix entre deux méthodes. Un : vous déterminez vous-même l'adresse de chaque PC. Deux : vous laissez la box internet attribuer une adresse aux PC qui lui sont connectés. Plus précisément, c'est le serveur DHCP de la box qui donne les adresses IP. Cette seconde méthode est plus facile à utiliser. Quelle que soit la méthode que vous choisissez, ouvrez *Centre Réseau et partage* du Panneau de configuration et cliquez sur le lien *Connexion au réseau local*. La boîte de dialogue *État de la connexion au réseau local*, cliquez sur le bouton *Propriétés*. Dans la liste des éléments, sélectionnez *Protocole Internet version 4* et cliquez sur *Propriétés*. Cochez l'option *Obtenir une adresse IP automatiquement*. Validez. Sur l'ordinateur Windows XP, ouvrez le dossier *Connexions réseau*. Cliquez du bouton droit sur l'icône de l'adaptateur réseau (Ethernet ou Wi-Fi) et choisissez la commande *Propriétés*. Dans la liste des protocoles, sélectionnez TCP/IP et cliquez sur le bouton *Propriétés*. Cochez l'option *Obtenir une adresse IP automatiquement*. Si le problème persiste, contrôlez dans les paramètres de la box si le serveur DHCP est activé (voyez le manuel de la box pour savoir comment accéder à son programme de configuration). ■

INTERNET

UTILISEZ DES FAX SANS TÉLÉCOPIEUR

Q ***Je n'ai pas de télécopieur. Est-ce que je peux quand même envoyer et recevoir des fax sur mon PC ?***

De Bruno Cambel

R Inscrivez-vous chez MonFax, un service en ligne de réception de fax gratuit. Dans la page d'accueil du site www.monfax.com, cliquez sur le bouton *Inscription*. Le formulaire d'inscription s'affiche. Choisissez une ville proche de chez vous afin de recevoir un numéro de fax. Il s'affiche immédiatement. Vous avez le choix entre un numéro surtaxé et un numéro gratuit. Les numéros géographiques (01, 02, 03, 04, 05) sont gratuits. Les numéros en 0826 sont surtaxés (15 centimes par minute). Pourquoi choisir un numéro surtaxé ? Pour éviter le spam. Beaucoup d'entreprises envoient de la publicité par fax. Généralement, elles évitent les numéros surtaxés. Complétez le reste du formulaire. Seules les données en rouge sont obligatoires. Cliquez sur le numéro de fax pour confirmer son ouverture. Votre numéro de fax est immédiatement opérationnel. Vous pouvez le communiquer à tous ceux qui veulent vous envoyer une télécopie. Un e-mail contenant votre numéro et votre mot de passe vous est immédiatement envoyé. Pour tester le service, envoyez-vous un fax. Pour cela, utilisez par exemple le service MyFax (www.myfax.com/free). Complétez le cadre *To* en indiquant votre numéro de fax. Dans le cadre *From*, entrez votre adresse e-mail. Pour envoyer un document précis, cliquez sur le bouton *Parcourir* dans le cadre *Fax Message*. Envoyez le fax avec le bouton *Send fax*. Un e-mail de confirmation vous est envoyé. Cliquez dans ce message sur le lien de confirmation. Votre navigateur vous informe que le fax a été envoyé. Vous recevrez un mail lorsque le fax sera envoyé. Le fax est réceptionné par MonFax qui vous le transmet, attaché à un e-mail. ■

OFFICE

WORD ET EXCEL SONT TROP LENTS

Q ***Lorsque j'ouvre une application Office en étant connecté à mon réseau, tout est normal. En revanche, lorsque j'essaie sans être connecté à mon réseau, le démarrage de l'application prend beaucoup de temps (environ 1 minute).***

De David Beni

R Au moment de leur démarrage, les applications de votre PC font appel à un élément installé quelque part sur le réseau. La recherche et l'activation de cet élément ralentissent l'ouverture des applications. Il est probable qu'il s'agisse de l'imprimante. Si le périphérique par défaut est connecté à un PC du réseau et partagé par celui-ci, il faut que le PC et l'imprimante soient allumés sinon les applications démarrent lentement car elles cherchent l'imprimante, sans le trouver. Si vous utilisez une imprimante réseau (Wi-Fi par exemple), il est possible que le pilote se trouve sur un autre PC de votre réseau. Installez ce pilote localement sur votre machine. Allumez l'imprimante et connectez votre PC au réseau. Dans le Panneau de configuration, ouvrez le module *Périphériques et imprimantes* (Windows 7) ou *Imprimantes* (Windows Vista). Cliquez sur *Ajouter une imprimante* puis sur *Ajouter une imprimante locale*. L'Assistant vous demande alors de choisir un port. Cochez *Créer un nouveau port* et dans la liste des types de port, cliquez sur *Standard TCP/IP Port* puis sur *Suivant*. Entrez l'adresse IP de l'imprimante et cliquez sur *Suivant*. Windows cherche le pilote et l'installe. Veillez à ce que l'imprimante par défaut soit bien celle que vous venez d'installer. ■

Release by TEAM-DZ

OFFICE
RESTRICTION

Q ***Lorsque je clique sur un lien dans un e-mail, j'obtiens le message : « Cette opération a été annulée à cause d'une restriction en vigueur sur cet ordinateur. Contactez votre administrateur système. » Je suis le seul à utiliser mon ordinateur et je suis l'administrateur.***

Jean-Pierre Laloux

R Dans la fenêtre d'Internet Explorer, choisissez la commande *Outils > Options Internet*. Passez à l'onglet *Programmes* et cliquez sur le bouton *Définir les programmes*. La fenêtre des programmes par défaut s'affiche. Cliquez sur *Définir les paramètres par défaut de l'accès aux programmes et de l'ordinateur*. Dans la fenêtre qui s'ouvre, cochez l'option *Microsoft Windows*. Les détails de la configuration Windows sont alors visibles. Assurez-vous que tout est correct (le navigateur, le programme de messagerie, le lecteur multimédia, la messagerie instantanée). Si la configuration affichée ne correspond pas à la réalité, cochez l'option *Personnaliser* et sélectionnez vous-même les logiciels. Validez avec *OK* puis fermez Internet Explorer. ■

AVIRA ANTIVIR
ÉCHEC DE LA DÉSINSTALLATION AUTOMATIQUE

Q ***J'ai essayé de désinstaller Avira AntiVir mais la procédure habituelle par le module*** **Programmes et fonctionnalités** ***du Panneau de configuration a échoué.***

De Marc Vrebos

R Puisque la désinstallation automatique ne fonctionne pas, voici la procédure pour le faire manuellement si vous avez la version 8 ou 9 d'Avira Antivir. Démarrez Windows en mode sans échec : relancez le PC et gardez pressée la touche [F8] jusqu'à ce que le menu de démarrage s'affiche. Appuyez sur le numéro correspondant au mode sans échec. Ouvrez l'Explorateur Windows et supprimez le dossier *C:\Programmes\AntiVir PersonalEdition*, *C:\Programmes\Avira Premium* ou *C:\Programmes\Avira*. Sélectionnez ensuite le dossier *C:\Documents and Settings\All Users\Application Data* (Windows XP) ou *C:\ProgramData* (Windows 7 ou Vista) et supprimez les dossiers dont le nom contient AntiVir ou Avira. Si le dossier Application Data n'est pas visible, choisissez (dans le menu de l'Explorateur Windows) la commande *Outils > Options des dossiers* (Windows XP) ou *Organiser >Options des données et de recherche* (Windows Vista ou 7). Dans l'onglet *Affichage* de la boîte de dialogue, cochez l'option *Afficher les fichiers, dossiers et lecteurs cachés*. Terminez la désinstallation en nettoyant la Base de registre avec l'utilitaire Registry Cleaner, fourni par Avira (http://dl.antivir.de/down/windows/registrycleaner_en.zip). ■

MATÉRIEL
UN DISQUE EXTERNE FANTÔME

Q ***Quand je branche un disque externe sur le port USB, Windows m'informe de sa reconnaissance, charge le pilote et me signale que le périphérique est opérationnel. Pourtant, il n'apparaît pas dans l'Explorateur Windows.***

De Paul Freney

R Il est probable que Windows ne parvienne pas à lui attribuer une lettre, ce qui le rend incapable de l'identifier en tant que lecteur et donc d'afficher son icône dans la fenêtre de l'Explorateur Windows. Renommez le lecteur correspondant au disque externe. Procédez ainsi : dans le Panneau de configuration, ouvrez le module *Outils d'administration* et double-cliquez sur *Gestion de l'ordinateur*. Cliquez, dans le volet gauche, sur *Gestion des disques*. Si un message d'alerte apparaît, c'est que votre disque USB n'est pas formaté ou qu'aucun volume n'a été créé. Laissez-vous guider par la procédure automatique de Windows. Sinon, cliquez du bouton droit su le nom de votre disque. Dans le menu contextuel, choisissez la commande *Modifier la lettre de lecteur et les chemins d'accès*. Cliquez sur le bouton *Modifier* et choisissez l'une des lettres proposées. Ouvrez à nouveau l'Explorateur Windows. L'icône du disque s'affiche. Profitez-en pour le nommer de manière significative. Cliquez dessus du bouton droit et choisissez la commande *Renommer*. ■

WINDOWS VISTA ET 7
CONFIGUREZ LA ZONE DE NOTIFICATION

Q ***À l'extrémité droite de la Barre des tâches, la flèche qui fait apparaître les icônes cachées a disparu. Comment la faire revenir ? Combien d'icônes cette zone peut-elle contenir ?***

De Clayette

R Par défaut, la zone de notification affiche les icônes que vous avez utilisées récemment. Les autres restent masquées et sont accessibles en cliquant sur la petite flèche que vous ne voyez pas sur votre PC. Pour configurer l'affichage des icônes dans cette zone, cliquez du bouton droit sur le bouton *Démarrer* (à l'extrémité gauche de la Barre des tâches) et choisissez la commande *Propriétés*. Dans la fenêtre qui s'ouvre, passez à l'onglet *Zone de notification*. Cochez les icônes système que vous voulez voir en permanence. Si l'option *Masquer les icônes inactives* n'est pas cochée, toutes les icônes seront visibles. Si l'option est cochée, seules les icônes fréquemment utilisées s'affichent. Cliquez sur le bouton *Personnaliser* pour forcer l'affichage des icônes de votre choix, quelle que soit leur fréquence d'utilisation. ■

Release by TEAM-DZ

HOTLINE

MATÉRIEL
UN GRAND CHOC

Q ***Mon ordinateur portable a subi un choc et, depuis lors, il ne démarre plus. Le disque dur semble en panne. Est-il possible de le récupérer ?***

De Marc Menton

R La plupart des ordinateurs portables peuvent encaisser sans dommage les petits heurts. Mais un choc trop violent provoque des traumatismes qu'il n'est pas toujours possible de réparer sans engager des frais trop importants. Si, en le démarrant, les voyants s'allument, mais l'écran reste noir, il est possible que les dégâts se limitent au disque dur. C'est en effet le composant le plus fragile de la machine. La face inférieure d'un ordinateur présente quelques ouvertures protégées par des plaques vissées. L'une de ces ouvertures donne accès au disque dur. Voyez si celui-ci est bien connecté. Si vous ne voyez rien d'anormal dans les câbles et les connecteurs, remplacez-le tout en sachant que ceci ne résoudra peut-être pas le problème. Dans le cas où le problème persiste, retournez votre matériel au fabricant – s'il est toujours sous garantie – ou trouvez un réparateur local. ■

MATÉRIEL
UN LECTEUR BIZARRE

Q ***Dès que j'ouvre ma session et chaque fois que j'accède à l'Explorateur Windows, un message d'erreur s'affiche. Il indique : « Il n'y a pas de disque dans le lecteur. Insérez un disque dans le lecteur \Device\Harddisk5\DR5 ».***

De Dominique Pinard

R Vérifiez les lettres de lecteur. Il est probable que Windows patauge dans l'attribution des lettres à un disque (externe ou interne), au lecteur de cartes mémoire ou encore aux ports USB. Ouvrez le module *Outils d'administration* du Panneau de configuration. Double-cliquez sur l'icône *Gestion de l'ordinateur*. Dans la fenêtre qui apparaît, ouvrez le dossier *Stockage/Gestion des disques*. Vérifiez la lettre de chaque lecteur. Veillez à ce que chaque lecteur ait une lettre différente. Contrôlez aussi la lettre du disque principal, qui doit être « C ». Redémarrez Windows. Si vous ne constatez aucune anomalie ou si les corrections apportées ne résolvent pas le problème, consultez le journal des événements. Procédez ainsi : dans le Panneau de configuration, ouvrez le module *Outils d'administration* et double-cliquez sur l'icône *Observateur d'événements*. Examinez les journaux Système et Application pour repérer l'événement étiqueté « erreur » en rapport avec le message qui s'affiche. Les explications de l'événement devraient vous aider à identifier l'élément responsable. ■

MULTIMÉDIA
LES BIBLIOTHÈQUES ITUNES

Q ***Ma bibliothèque musicale iTunes contient plus de 2000 morceaux. Je voudrais la diviser en deux ou trois, mais je ne trouve aucune commande pour le faire. Est-ce possible ?***

De M. Pereira

R Quittez *iTunes*. Ouvrez le menu *Démarrer* et lancez *iTunes* tout en appuyant sur la touche [Maj]. Un message vous propose de choisir ou de créer une bibliothèque. Cliquez sur le bouton de création. Attribuez à la bibliothèque un nom significatif. Ensuite, il suffira d'importer les morceaux que vous souhaitez inclure dans cette bibliothèque : utilisez la commande *Ajouter le fichier* ou *Ajouter le dossier* dans le menu *Fichier*. iTunes ouvre la dernière bibliothèque utilisée, à moins que vous ne pressiez la touche [Maj] pour en choisir une autre. ■

WINDOWS
CLÉ IMPOSSIBLE À SUPPRIMER

Q ***Je voudrais supprimer une clé de la Base de registre dans la fenêtre de regedit. Mais c'est impossible. J'obtiens le message suivant : « Erreur lors de la suppression de la clé ».***

De Philippe Guiche

R Il est possible que cette clé soit utilisée par un logiciel en cours de fonctionnement. Quittez tous les logiciels et essayez à nouveau. Si la suppression est toujours impossible, redémarrez en mode sans échec, lancez *regedit* et essayez de supprimer la clé. Ça ne marche pas ? Redémarrez en mode normal. Ouvrez *regedit* et cliquez du bouton droit sur la clé à supprimer. Dans le menu contextuel, choisissez la commande *Autorisations*. Si le groupe *Tout le monde* n'est pas visible dans la liste, cliquez sur *Ajouter*. La fenêtre *Sélectionnez utilisateurs ou groupes* s'affiche. Cliquez sur *Avancé*. Dans la nouvelle fenêtre, cliquez sur *Rechercher*. Dans les résultats de la recherche, diquez sur *Tout le monde* puis sur le bouton *OK*. Validez en cliquant à nouveau sur le bouton *OK*. De retour dans la fenêtre des autorisations, sélectionnez *Tout le monde* et cochez l'option de contrôle total dans la colonne *Autoriser*. Fermez la fenêtre en cliquant sur *OK*. Vous pouvez maintenant supprimer la clé. ■

COMPTABILITÉ
REMPLACEZ MICROSOFT MONEY

Q ***J'utilise Microsoft Money depuis longtemps. Malheureusement, Microsoft n'a pas jugé bon de continuer à fournir le logiciel en version française. J'ai plusieurs années d'archives. Il est donc important pour moi de continuer avec le même produit ou un très proche de Money. Quels sont les produits qui pourraient remplacer Money avantageusement ?***

De Gérard Antoine

R Remplacez Money par Money Manager (http://money-manager.softonic.fr/telecharger), un logiciel gratuit et traduit en français. Il importe les données Excel au format CSV ainsi que les fichiers QIF générés par Quicken et Microsoft Money. Il gère tous les types de comptes, les chèques, les cartes de crédit, les investissements. Money Manager facilite les prévisions budgétaires ainsi que la gestion des factures et des paiements. Mais il ne rapatrie pas les données de votre compte bancaire en ligne. Si la connexion à votre compte bancaire s'avère importante, choisissez plutôt Quicken (en vente dans les magasins d'informatique habituels). Autre solution : AceMoney (www.mechcad.net/downloads). Ce logiciel est proposé en plusieurs versions payantes (avec une période d'essai de trente jours). Il existe également une version totalement gratuite. ■

Release by TEAM-DZ

OUTLOOK
IMPORTATION

Q ***Je n'arrive pas à importer dans Outlook les contacts de Windows Live Mail. Tout se déroule apparemment sans problème, mais les données sont inexploitables !***

De S. Mousse

R Le problème, c'est le format du fichier CSV. Windows Live Mail crée un fichier dans lequel les données sont séparées par un point-virgule et Outlook s'attend à ce que, dans le fichier CSV, les données soient séparées par une virgule. La solution consiste à remplacer les points-virgules par des virgules. Cliquez du bouton droit sur l'icône du fichier exporté et, dans le menu contextuel, cliquez sur *Ouvrir* avec le bloc-notes. Choisissez la commande *Édition > Remplacer* pour effectuer les changements. ■

MESSAGERIE
SAUVEGARDEZ SANS EXPORTER

Q ***J'ai lu dans votre numéro d'avril le moyen de sauvegarder les données d'Outlook. Je voudrais savoir s'il est possible de synchroniser directement certains dossiers sans passer par leur exportation ?***

De Pascal Jumel

R Inscrivez-vous par exemple chez MobileMe, un service en ligne signé Apple, qui propose un espace de stockage pour des fichiers ainsi que pour le courrier, le calendrier, les contacts d'Outlook. En installant un utilitaire de connexion, vous pourrez synchroniser plusieurs machines afin que toute modification apportée sur l'une d'elles soit automatiquement répercutée dans votre espace en ligne et sur tous les autres appareils. Ainsi, un rendez-vous créé sur votre iPhone sera transféré en quelques minutes sur votre PC à la maison. Pour créer un compte, accédez à www.mobileme.com à partir d'un PC (de préférence avec Firefox). Cliquez sur le lien *En savoir plus* dans la case *Essai gratuit*. Vous avez droit à soixante jours gratuits. Après cette période, vous devrez vous abonner.

Il semble qu'Apple va annoncer prochainement la gratuité totale de MobileMe. Mais jusqu'à présent, il s'agit seulement d'une rumeur. Téléchargez le module MobileMe à l'adresse http://support.apple.com/ downloads/DL769/en_US/MobileMeSetup.exe. Démarrez-le et connectez-vous à MobileMe en indiquant vos identifiants : nom de membre et mot de passe. Cliquez sur *Se connecter*. La fenêtre du module contient maintenant trois onglets. Cliquez sur *Synchroniser* et cochez l'option *Synchroniser avec MobileMe*. Vous avez le choix du rythme de la synchronisation. Si vous optez pour *Automatiquement*, les données seront synchronisées chaque fois qu'il y aura un changement sur le PC et chaque fois que vous ouvrirez un dossier contenant des données synchronisées.

Si vous consultez le calendrier, par exemple, Outlook contrôle si MobileMe a enregistré des mises à jour. Celles-ci sont alors importées. Choisissez les données qui seront synchronisées et le logiciel de référence. Par exemple : le calendrier d'Outlook. Cliquez sur le bouton *Synchroniser* pour effectuer l'opération une première fois. Un message vous demande de sélectionner une action. Choisissez *Remplacer les données sur MobileMe*. Validez avec le bouton *Autoriser*. Les données sont transférées vers MobileMe. ■

MATÉRIEL
8 GO DE MÉMOIRE VIVE

Q ***Je viens d'installer 4 Go supplémentaires de mémoire vive. Mon PC Windows 7 possède donc maintenant 8 Go. Que faut-il paramétrer pour bénéficier pleinement de cette augmentation de mémoire ?***

De Marc Éric

R Les versions 32 bits de Windows 7 reconnaissent au maximum 4 Go de mémoire vive. Les versions 64 bits Utimate, Entreprise et Professionnelle reconnaissent jusqu'à 192 Go… Windows utilise toute la mémoire vive qu'il peut gérer. Si vous installez 8 Go de RAM sur un PC Windows 7 32 bits, seuls les 4 premiers Go seront utilisés. Le surplus est tout simplement ignoré. Par ailleurs, le passage de 4 à 8 Go sur un système 64 bits accélère le multitâche, le basculement entre applications et le fonctionnement général du PC. Dans des conditions normales d'utilisation, cette accélération n'est pas vraiment spectaculaire. En revanche, les applications qui gèrent de grandes quantités de données sont plus rapides. Pour que Windows gère toute la RAM disponible, il faut configurer le Bios. Redémarrez le PC et appuyez sur la touche qui ouvre le setup (le programme de configuration du Bios). Recherchez un paramètre nommé par exemple Memory Remap (le nom varie selon les Bios) et activez-le. ■

WINDOWS 7
32 OU 64 BITS ?

Q ***Je veux remplacer mon ordinateur Windows XP. J'ai donc le choix entre Windows 7 32 bits ou 64 bits. Comment décider ?***

De Daniel Falandry

R Les termes 32 bits et 64 bits concernent la manière dont le processeur traite les données. La version 64 bits de Windows est capable de gérer une grande quantité de mémoire vive de manière plus efficace qu'un système 32 bits. La plupart des programmes conçus pour la version 32 bits de Windows fonctionnent sur la version 64 bits. Il y a cependant des exceptions pour quelques antivirus et utilitaires système. En revanche, les pilotes de périphériques élaborés pour la version 32 bits de Windows ne fonctionnent pas ou mal sous une version 64 bits. Voyez sur le site des fabricants de vos périphériques s'ils proposent un pilote 64 bits. Passez par le site www.touslesdrivers.com pour vous aider à accéder à la page des pilotes des fabricants. En règle générale, recherchez les produits (logiciels et périphériques) qui affichent le logo « Compatible Windows 7 ». Ils ont été testés pour être compatibles avec les versions 32 et 64 bits de Windows 7. Vous pouvez également consulter le site *http://go.microsoft.com/fwlink/?linkid=160679* pour accéder à la page de Microsoft et rechercher le Centre de compatibilité Windows 7 (www.microsoft.com/windows/ compatibility/windows-7/fr-fr). Mais l'absence d'un produit dans la liste ne signifie pas qu'il ne soit pas compatible avec Windows 7. Il faut aussi tenir compte du fait que l'installation d'une version 64 bits sur un PC exécutant une version 32 bits exige le formatage du disque dur, et donc la réinstallation de tous les logiciels et la sauvegarde préalable de vos fichiers. Si vous achetez un ordinateur Windows 64 bits, vous le ferez évoluer sans souci vers la prochaine version de Windows 64 bits. ■

Release by TEAM-DZ

WINDOWS
VOIR LES MINIATURES

Q ***L'Explorateur de Windows 7 n'affiche pas les miniatures des fichiers PDF et PSD (Photoshop). J'ai des centaines de ces fichiers. Comment afficher des miniatures ?***

De Stéphane Fernandes

R Windows 7 affiche la miniature d'un grand nombre de types de fichiers, mais il ignore les fichiers PSD et PDF. Ce n'est pas inéluctable. Installez *KaSaLong Thumbnails*, un petit programme qui active les miniatures pour six types de fichiers : AI (Illustrator Vector Graphic), PSD (Photoshop), CDR (Corel Vector Graphic Drawing), EPS (Encapsulated PostScript), TGA (Truevision Targa Graphic), ICL (Icon Library File). Il est gratuit et compatible avec toutes les versions de Windows 32 et 64 bits. Téléchargez-le ici : http://download.phpstory.com/KaSaLong.Thumbnails.exe. Pour afficher les miniatures PDF, Targa, Raw, Google Sketchup, JPEG 2000, installez plutôt Mystic Thumbs. Téléchargez la version d'essai (30 jours) : www.mysticcoder.net/mysticthumbs.html. Installez la version 32 ou 64 bits selon le système de votre PC. ■

MESSAGERIE
PIÈCES JOINTES ILLISIBLES

Q ***Depuis quelque temps, je ne peux plus voir le contenu de certaines pièces jointes. Un message m'informe qu'Adobe Reader n'a pas pu ouvrir le fichier, car son type n'est pas pris en charge ou le fichier est endommagé. Que faire pour retrouver comme avant l'ouverture d'un simple clic ?***

De Jean Sourie

R Lorsque vous cliquez sur une pièce jointe pour voir son contenu, Windows détecte le type de fichier et lance le programme qui lui est associé. Par exemple, si vous recevez un fichier MP3, Windows ouvre le lecteur Windows Media ou un autre logiciel audio qui vous fait alors entendre la musique. Chez vous, ce système ne fonctionne plus. Il y a deux explications possibles : le fichier que vous avez reçu est endommagé ou le logiciel habilité à afficher le contenu de ce fichier n'existe pas. La première explication est à exclure si le problème se manifeste à plusieurs reprises, pour des fichiers différents. Dans votre cas, vous recevez des fichiers PDF et Windows cherche le programme de lecture des fichiers PDF : Adobe Reader. Il ne le trouve pas ou, s'il le trouve, ne parvient pas à le lancer. Réinstallez Adobe Reader : dans votre navigateur internet, entrez l'adresse www.adobe.com/fr/products/acrobat/readstep2.html. Dans la page qui s'affiche, décochez l'option *Barre d'outils Google gratuite* et cliquez sur le bouton *Télécharger dès maintenant*. Suivez les instructions de téléchargement et d'installation. ■

VIDÉO
LA LECTURE DE FICHIERS PVR

Q ***Comment lire des films enregistrés sur une clé USB ou un disque dur au format PVR, pour les regarder ensuite sur un téléviseur via une passerelle qui accepte uniquement les fichiers AVI, MPEG et XviD ?***

De Jean Febvay

R Si les fichiers PVR portent l'extension .TS (c'est par exemple le cas des enregistrements vidéos sur la Freebox HD), convertissez-les en DivX ou XviD avec AutoGK (www.autogk.me.uk). Son point fort, c'est l'automatisation de son paramétrage. Après avoir choisi le fichier source, il suffit de sélectionner la ou les pistes sonores, la taille attendue du fichier cible et le tour est joué. Il détecte automatiquement les meilleurs paramétrages pour créer le fichier désiré. Voyez le tutoriel en français : www.autogk.me.uk/modules.php?name=TutorialFR. Si les fichiers portent l'extension PVR, essayez simplement de leur attribuer l'extension .AVI. Par ailleurs, pour voir des vidéos .PVR sur un ordinateur, utilisez le logiciel VLC (www.videolan.org/vlc). ■

STOCKAGE
CLASSEZ ET ORGANISEZ LES CD-R

Q ***Comment procéder au classement et à l'organisation de mes CD-R (disques compacts enregistrables) ?***

De Georges Berthou

R AACD (**http://aacd.softonic.fr/telecharger**) indexe le contenu de vos CD, mais aussi celui de vos DVD, de vos clés USB et de vos disques externes. Une fois que c'est fait, il affiche leur contenu sans que le support ne soit physiquement présent dans un lecteur ou connecté à l'ordinateur. Une barre d'outils permet d'afficher les miniatures des images, les informations des fichiers MP3 et le contenu des fichiers textuels. Outre la présentation standard sous une forme arborescente, vous pourrez créer des conteneurs représentant les espaces de rangement où sont effectivement stockés vos CD. Avec le module de recherche, vous retrouverez facilement n'importe quel fichier : le logiciel indique alors le disque compact sur lequel il est stocké. Le logiciel est en français, facile à maîtriser et surtout... gratuit. ■

Release by TEAM-DZ

EN VENTE ACTUELLEMENT

5,90 € seulement

www.microactuel.com

HS N°7 JUIN/JUILLET 2011

CD-ROM GRATUIT

micro actuel

200 PAGES DE FICHES PRATIQUES

• **Suivez** tous vos réseaux sociaux d'un seul coup P. 89

• **Imprimez** directement une page web P. 131

METTEZ tous vos fichiers à l'abri P. 103

COMMENT...
✔ Stocker vos données en ligne
✔ Les sécuriser sur votre disque dur

INSTALLEZ et configurez un tuner TNT P. 139

CRÉEZ et partagez gratis vos données P. 107

DEVENEZ un as de BING ! P. 117

• **Sauvegardez** toutes vos données Outlook P. 69

• **Surfez** discrètement avec Google Chrome P. 75

• **Personnalisez** le bureau de Windows 7 P. 163

• **Prenez** de belles photos avec votre iPhone P. 179

• **Connectez** des accessoires à l'iPad P. 147

GARDEZ VOTRE PC À JOUR P.149

Tous nos conseils pour...
✔ Analyser ses composants
✔ Changer les éléments vieillissants

FRANCE MÉTROPOLE : 5,90 € – BELGIQUE : 7,00 € – DOM : 7,00 €
CANADA : 11,25 $ CAN – MAROC : 80 DH – SUISSE : 12 CHF

60 LOGICIELS ESSENTIELS POUR OPTIMISER ET SÉCURISER VOTRE PC

Release by TEAM-DZ

Les données de votre entreprise sont-elles bien protégées ?

Eaton, leader mondial en Protection électrique.

Foudre, coupures, surtensions ... vos données et votre matériel informatique courent des risques à chaque instant. Offrez leur la meilleure protection : **les onduleurs et multiprises parafoudres Eaton.**

www.eaton.fr/powerquality

onduleurfrance@eaton.com