

TOUS LES LOGICIELS DE SURVEILLANCE EXPLIQUÉS PAS À PAS

HACKERS

MAGAZINE

SUR LE CD

**120 LOGICIELS
GRATUITS !**

ANONYMAT, ENCRYPTAGE,
NAVIGATEUR & EMAIL,
COPIE, MOT DE PASSE, P2P,
PROGRAMMATION, SNIFFER,
SYSTÈME, TUTO,
UTILITAIRES SÉCURITÉ...

**SPECIAL
HARDWARE**

Les kits complets
POUR ESPIONNER
à la maison et ailleurs...

**TOUT POUR ÊTRE UN
VÉRITABLE ESPION**

Tous **LES LOGICIELS INDISPENSABLES** pour **ESPIONNER**

RELIGIÖSE/LUXEMBOURG, 5,5€ - SUISSE, 9,9€ - AUTON., 8,00 CHF
DOM., 5,5€ - HARGOC, 6,00 MAD



WLF
PUBLISHING

HACKERSMAGAZINE

3ème année - N° 24

Juillet/Août 2008

Prix affiché : 4.99 €

son CD-ROM exclusif

Ne peut être vendu séparément

Hackers Magazine

est un journal européen et canadien

Réalisé par une communauté

cosmopolite principalement

française, italienne et québécoise

Les joyeux hackers de la

Rédaction :

Greg. E., Muppy, Eric Deloize

One 4 Bus, Walter Grossebaume, Oku,

Orange Group, Ferluc,

Editeur :

WLF Publishing SRL

Via Donatello 71

00196 Roma

Imprimeur :

Roto 2000

Via Leonardo Da Vinci 18/20

Casarin (MI) Italie

Distributeur :

NMPP

ISBN : en cours

Dépôt légal : à parution

Directeur de la publication :

Teresa Carsaniga

Tout le contenu est open source uniquement pour une utilisation en ligne avec une référence au magazine. La rédaction n'est pas responsable des textes, photos, illustrations et dessins qui engagent la seule responsabilité de leurs auteurs. Sauf accord particulier, les manuscrits, photos et dessins adressés à Hackers Magazine publiés ou non, ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire. Tous droits réservés Hackers Magazine 2008

AU PAYS DE L'HADOPI...

Comme dans tous les pays, on poursuit, on traque, on leurre, Il y a des méchants et des hackers...

En validant, le 12 juin dernier, le projet de loi Hadopi - pudiquement appelé « Création et Internet » par le gouvernement -, le Conseil d'Etat a ouvert la porte à l'adoption de ce nouveau texte législatif réprimant le libre usage des ressources numériques. Bien entendu, la riposte graduée retenue par ce dispositif (double avertissement par mail et lettre recommandée avant résiliation forcée de l'abonnement Internet du contrevenant) pour punir les internautes insoumis est mille fois moins scandaleuse que la logique répressive actuelle (jusqu'à 300 000 euros d'amende et 3 ans de prison selon l'article L335-2-1 du code de la propriété intellectuelle). Néanmoins, le champ des libertés se restreint encore un peu. En fait, le gouvernement semble adapter le modèle répressif du foot au web. De la même façon qu'il y a des « Interdits de stade » (IDS en langage ultra), il y aura demain des « Interdits de web ». Et nous, à Hackers Magazine, on sera toujours du côté des dissidents.

La rédaction

» SOMMAIRE

SPYWARE

MAIS OÙ SE CACHENT-ILS? **PAG. 03**

SPYING TOOLS

TRAQUEZ LES ESPIONS! **PAG. 16**

KEYLOGGER

SÉCURISEZ VOTRE ORDINATEUR **PAG. 06**

MOBILE SPYING

TELEPHONE ESPION **PAG. 22**

FIREWALL

UN MUR INFRANCHISSABLE? **PAG. 08**

PORT SCANNER

ADVANCED PORT SCANNER 13 **PAG. 24**

ANTIVIRUS

MAIS PAS SEULEMENT! **PAG. 10**

PASSWORD CRACKING

JOHN THE RIPPER **PAG. 26**

REMOTE CONTROLL

AVEC LOGMEIN, VOTRE ORDINATEUR VOUS SUIT PARTOUT **PAG. 12**

CRYPTING

CRYPTOCO **PAG. 28**

ANTIROOTKIT

ANTIROOTKIT **PAG. 14**

STEGANO

MP3STEGO **PAG. 30**

SUR LE CD DE HACKERS MAGAZINE 24:

ANONYMAT

- ▶ ANONYMITY 4 PROXY 2.8
- ▶ CCLEANER 1.41.544
- ▶ GETANONYMOUS 2.2
- ▶ GHOSTSURF PLATINUM 3.0
- ▶ IE PRIVACY KEEPER 2.7.3
- ▶ JACK B. NYMBLE 2.1.4
- ▶ JAP ANONIMITY & PRIVACY
- ▶ MULTIPROXY 1.2
- ▶ TOR 0.1.0.15

NAVIGATEUR & MAIL

- ▶ AMAZECOPY 1.4
- ▶ CALLINGID TOOLBAR 1.6.0.6
- ▶ FIREFOX 2.0.0.4
- ▶ FIREFOX PORTABLE
- ▶ FIRSTSTOP WEBSEARCH
- ▶ FLOCK FOR WINDOWS 0.9.0.0
- ▶ MAGIC BOOKMARKS 1.03B
- ▶ MOBILE TCP 1.2
- ▶ PICTURES TOOLBAR
- ▶ THUNDERBIRD 2.0

CRYPTAGE

- ▶ AXCRIPT 1.6.3
- ▶ CRYPTAINER LE
- ▶ GHOSTPHRASE 2.5
- ▶ INVISIBLE SECRETS 4
- ▶ IOPUS SECURE EMAIL
- ▶ KRUPTOS 2.3
- ▶ PUFF 1.01
- ▶ SECURE FTP 2.5.13
- ▶ SECURETASK 2.0
- ▶ TRUECRYPT 4.3A
- ▶ VOICEMASK PRO

COPIER

- ▶ CDBURNERXP PRO 3.0.116
- ▶ DEEPBURNER PORTABLE 1.8
- ▶ FINALBURNER FREE 1.16.0.90
- ▶ FREE EASY CD DVD BURNER
- ▶ GRAB&BURN 5.0.2
- ▶ IGNITION 2.11.1.54
- ▶ IMGBURN 2.3.2.0
- ▶ SC DVD COPIER
- ▶ SIMPLY SAFE BACKUP

PASSWORD

- ▶ ABF PASSWORD RECOVERY 1.7.4.11
- ▶ ASTERISK LOGGER 1.2
- ▶ FOLDER PASSWORD EXPERT
- ▶ GUAPDF 2.3
- ▶ KEEPASS PASSWORD SAFE 1.07
- ▶ MAIL PASSWORD RECOVERY V1.1
- ▶ MY SECRET BOOKMARKS
- ▶ PASSWORD AGENT LITE 2.5.1
- ▶ PASSWORD SPECTATOR LITE 3.2
- ▶ PDF PASSWORD REMOVER 3.0

P2P

- ▶ AZUREUS 3.0
- ▶ BITCOMET 0.90
- ▶ BITTORRENT 5.07
- ▶ BUFFERZONE SECURITY FOR P2P FILE SHARING 2.10-37
- ▶ EMULE 0.49A
- ▶ SHAREAZA 2.2.5
- ▶ SWAPPER 1.0.4
- ▶ TRUSTYFILES FREE 3.1.0.18
- ▶ WINMX 3.0.3.54B4
- ▶ XNAP 2.5R3

PROGRAMMATION

- ▶ CSE HTML VALIDATOR LITE 8.04
- ▶ EMS SQL MANAGER 2007 LITE
- ▶ EXCELSIOR INSTALLER 1.1
- ▶ IISPASSWORD 1.0
- ▶ JAVA TOOLS 0.29
- ▶ LINE COUNTER 1.03
- ▶ RIGHTWEBPAGE 0.5.6
- ▶ WEB CEO FREE EDITION 6.5
- ▶ WEBLOG EXPERT LITE 4.1
- ▶ XMLSPEAR 2.3

SÉCURITÉ

- ▶ AD-AWARE 2007 FREE
- ▶ AVAST! HOME EDITION 4.7.892
- ▶ COMODO FIREWALL 2.4
- ▶ CWSHREDDER 2.19
- ▶ PHISHGUARD FOR IE 2.1.131
- ▶ POPFILE 0.22.4
- ▶ SANDIEBOX 3.0
- ▶ SMART DATA RECOVERY
- ▶ SPYBOT SEARCH&DESTROY 1.4
- ▶ SPYWARE TERMINATOR 1.9.3.142

SNIFFER

- ▶ AIRSNARE 1.5
- ▶ ETHEREAL NETWORK ANALYZER
- ▶ INFILTRATOR NETWORK SECURITY SCANNER 3.0
- ▶ IP SNIFFER 1.91
- ▶ NETWORK STUMBLER 0.4.0
- ▶ NETWORKACTIV PIAFACTM 2.0
- ▶ NMAPWIN 1.2.3
- ▶ PROXY SNIFFER FREE EDITION 3.1-A
- ▶ SNIFFPASS 1.01

SYSTÈME

- ▶ BOOT BUILDER
- ▶ DRIVERMAX 2.4
- ▶ FRESH UI 7.83
- ▶ HDCLEANER 2.364
- ▶ KILLPROCESS 2.42
- ▶ OPENEDFILESVIEW 1.02
- ▶ PCBASELINE 1.0.3
- ▶ QUICK STARTUP 2.0
- ▶ WINAUDIT 2.18
- ▶ XP TCP/IP REPAIR 1

TUTORIEL

- ▶ ADVANCED PORT SCANNER
- ▶ AVAST
- ▶ HIJACKTHIS
- ▶ JOHN THE RIPPER
- ▶ KGB FREE KEYLOGGER
- ▶ LOGMEIN
- ▶ MP3STEGO
- ▶ CRYPTOCD
- ▶ SOPHOS
- ▶ ZONE ALARM

UTILITAIRES

- ▶ 7-ZIP
- ▶ ACROBAT READER 8
- ▶ DIVX PLAY BUNDLE 6.6
- ▶ HTRACK WEBSITE COPIER
- ▶ JAVA 2
- ▶ RJJEXTENSIONS
- ▶ SAM SPADE
- ▶ SMARTFTP
- ▶ TREESIZE
- ▶ XNVIEW 1.91

MAIS OÙ SE CACHENT-ILS ?

Grâce à ce petit programme gratuit, découvrez quels sont les processus actifs sur votre ordinateur et localisez les indésirables.

Lorsque vous utilisez votre ordinateur, des dizaines de processus fonctionnent en continu sans que vous vous en rendiez compte. Il s'agit presque toujours de composants utiles, ou du moins inoffensifs, mais pouvant toutefois dissimuler une menace pour votre sécurité. Pour ne pas être pris au dépourvu, utilisez HijackThis, la performance à l'état pur !

■ L'ŒUVRE D'UN PASSIONNÉ

Développé au départ en tant que freeware par un maniaque de la sécurité, HijackThis est très rapidement devenu l'un des outils incontournables de la collection de softwares de tout hacker qui se respecte. Le succès de ce programme a également ravivé l'intérêt des grosses sociétés. Et ce n'est pas un hasard si la version la plus récente d'HijackThis (la 2.0.2), est aujourd'hui directement proposée par Trend Micro, par chance toujours gratuitement. Vous pouvez la télécharger directement sur le site www.trendsecure.com et l'installer sur votre ordinateur pour commencer à l'utiliser au plus vite.

■ A LA CHASSE AUX INTRUS !

Ce software fonctionne très simplement, du moins en théorie : il vérifie tous les processus actifs sur votre ordinateur, en analysant en profondeur les paramètres et données du Registre système. Si vous êtes patient, vous pouvez ensuite les examiner un

à un, pour vérifier si toutes ces opérations sont licites et si elles ne cachent pas quelques malwares. En outre, il s'agit-là d'un excellent outil pour traquer tous ces softwares qui, à votre insu, utilisent des ressources système, afin de les supprimer une bonne fois pour toutes.

Vous pouvez étudier manuellement les résultats des analyses d'HijackThis ou, si vous préférez, recourir à l'un des nombreux sites créés par les passionnés pour soutenir ce programme : dans ce dernier cas, il vous suffit de télécharger le fichier log sur l'un des forums spécialisés et attendre qu'un expert en sécurité vous donne son verdict, en vous suggérant d'intervenir ou non, et si oui, par quels moyens pour renforcer la sécurité de votre ordinateur.

■ PRENEZ GARDE

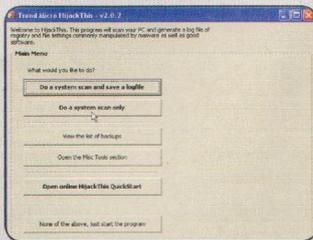
HijackThis est un outil particulièrement efficace dans la lutte contre les malwares ou tout simplement contre ces programmes "voleurs de ressources". Vous devez toutefois prêter garde pendant son utilisation, car l'exclusion de certains processus fondamentaux de Windows pourrait compromettre le

fonctionnement du système d'exploitation. Après avoir effectué un scan avec ce software, vous pouvez localiser tous les processus dont la nature vous inquiète, puis effectuer une simple recherche sur Google, en tapant en entier le nom du processus entre guillemets. Vous pourrez ainsi facilement découvrir si vous avez affaire à une fonction normale de Windows ou de quelques programmes, ou bien à un malware ou à un programme indésirable qui vous fait perdre des ressources, et agir en conséquence.

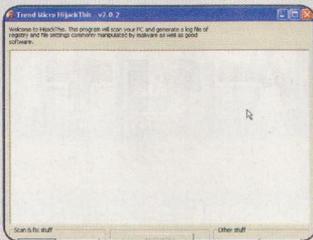


TUTORIAL

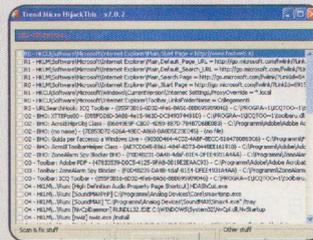
SPYWARE



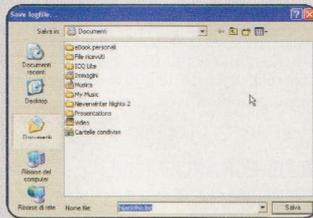
1 Première fenêtre
Lorsque vous lancez le programme, vous pouvez effectuer un choix parmi les fonctions principales. Dès le premier lancement, nous vous conseillons de lancer un scan du système avec do a system scan and save a log file.



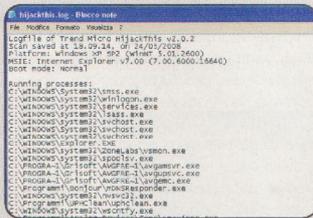
2 Essentielle et pratique
La partie graphique n'est certes pas celle sur laquelle les programmeurs ont passé le plus de temps, mais le résultat est très fonctionnel : cliquez sur la touche Scan, en bas à gauche, pour lancer une analyse du système.



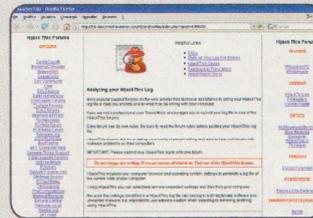
3 Perdu ?
Le résultat du premier scan se traduit inévitablement par une longue liste de processus et de fonctions. Pas de panique ! Généralement, il s'agit d'éléments faisant partie de Windows ou d'autres programmes.



4 Enregistrez le log
Une fois le scan achevé, vous pouvez créer une copie du fichier log sur votre disque dur. Elle vous sera utile tant pour contrôler, plus tard, les éléments modifiés sur votre ordinateur, que pour demander des conseils aux experts sur les différents forums.



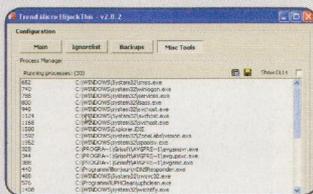
5 Informations utiles
Le fichier log vous présentera une liste de processus, en vous montrant la position du fichier exécutable qui les a générés. A ce stade, vous pourrez déjà détecter d'éventuelles anomalies.



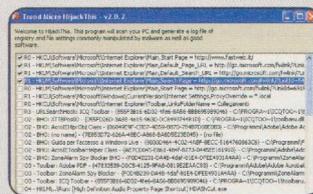
6 Experts : help !
Il existe différents sites et forums sur lesquels vous pouvez télécharger le fichier log d'HijackThis pour obtenir un avis sur l'état de santé et la sécurité de votre PC. Vous pourrez en trouver une liste sur <http://hjt-data.trend-braintree.com>.



7 Lire le scan
L'analyse effectuée par HijackThis présente une liste de processus, précédés d'un sigle. Vous pourrez trouver une explication de ce sigle sur le site www.castlecoops.com, dans la section HijackThis, pour distinguer immédiatement les processus inoffensifs.



8 Des analyses, mais pas seulement !
Parmi les outils d'HijackThis, vous trouverez également une fonction semblable au Gestionnaire de ressources Windows, qui vous permettra de terminer les processus actifs. Pour l'activer, sélectionnez Config dans la fenêtre principale puis



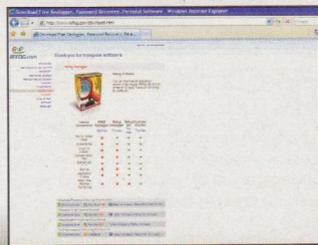
9 Fausse alertes
En utilisant HijackThis, apprenez à reconnaître les processus inoffensifs. Pour faciliter le travail du programme, sélectionnez-les puis cliquez sur Add checked to ignore list : dès lors, ils ne seront plus détectés lors des prochains scans.

SÉCURISEZ VOTRE ORDINATEUR

La dernière version de KGB Free Keylogger intègre davantage de fonctions, toutes plus efficaces les unes que les autres, pour intercepter les frappes sur le clavier de l'ordinateur sur lequel il est installé. Utile pour vérifier toute utilisation ou abus perpétré sur votre PC à votre insu. Essentiel aussi pour récupérer des travaux non enregistrés en cas de bug du système.

Savoir qui utilise votre PC à votre insu et ce qu'il en fait, est déjà en soi un excellent motif pour installer KGB Free Keylogger, récemment proposé par Refog dans sa version 4.5.5.836. Surtout pour effectuer un contrôle parental sur l'activité de vos bout'choux un peu trop curieux, ou encore sécuriser certaines activités professionnelles prévoyant l'archivage de données sensibles sur votre ordinateur. Mais l'utilisation de Keylogger s'avère tout aussi indispensable pour enregistrer les documents tapés et non encore enregistrés si le système bugue, dans la mesure où il permet d'intercepter tout ce qui a été tapé sur le clavier.

Cette fonction de base est disponible sur la version gratuite du software, que vous pouvez télécharger sur une page web spécifique du développeur, à l'adresse www.refog.com, comme indiqué à la Fig. 1.

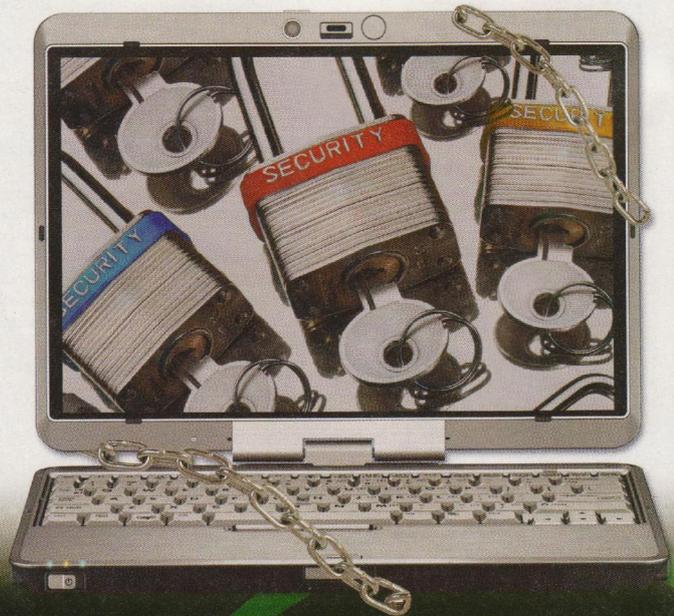


Pour ceux qui souhaitent bénéficier d'un contrôle renforcé sur leur machine, voici des produits plus complets, comme Key Logger, proposé à 39,00 €, qui devient invisible, même sur la liste des processus, et qui peut enregistrer aussi les fenêtres affichées à l'écran ; Spy, qui permet d'envoyer en toute discrétion des logs par e-mail et FTP, intègre quant à lui des alarmes et autres filtres sur des applications

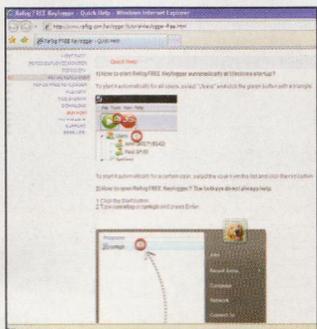
spécifiques (69,00 €). Enfin, Employee Monitor inclut le contrôle distant pour un prix public de 189,00 € comprenant cinq licences d'utilisation.

■ TÉLÉCHARGEMENT ET INSTALLATION

Téléchargez le fichier et enregistrez l'exécutable `Free_refog_setup_455`.



exe sur votre ordinateur. Lancez l'exécutable en confirmant le message qui s'affiche dans la fenêtre de notification et paramétrez la langue d'installation. Actuellement, seuls l'anglais, l'allemand et l'espagnol sont disponibles : nous vous conseillons donc de choisir l'anglais pour plus de praticité. A présent, le wizard se lance pour la configuration guidée de KGB Free Keylogger, en vous invitant à fermer les autres applications éventuellement actives sur votre PC. Les fenêtres suivantes affichent une comparaison entre les fonctions des différents produits Refog, sans oublier le sempiternel contrat de licence. A la fin de la procédure, en choisissant de lancer le programme et le système d'aide QuickHelp, sélectionnables à partir des fenêtres spéciales, vous serez redirigés vers la page d'aide de Refog, comme indiqué à la Fig. 2.



■ LANCEZ FREE KEYLOGGER

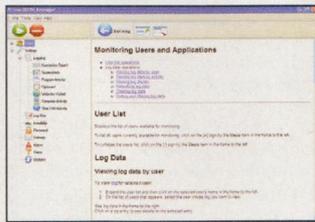
Une fois le programme lancé, avec son icône installée automatiquement dans la barre des tâches sur le bureau, vous verrez apparaître une fenêtre avec un message vous proposant d'upgrader un produit Refog pour obtenir des fonctions supplémentaires (et payantes), télécharger Free Refog Keylogger (déjà fait) ou encore lancer l'interface du programme en cliquant sur Ok, comme montré à la Figure 3.

Les deux liens situés dans la partie inférieure vous permettent en outre de revenir à la Page d'accueil de Refog.com ou d'accéder à la rubrique d'Aide.



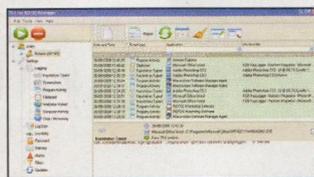
■ L'UTILISATION DU PROGRAMME ET DES CONCEPTS DE BASE

La fenêtre d'interface principale de Free Keylogger offre une vue d'ensemble des fonctionnalités du programme, à savoir les outils spécifiques pour effectuer les actions nécessaires. L'anglais étant l'une des seules langues disponibles, certains pourraient avoir un peu de mal à se familiariser aux commandes spécifiques, mais l'interface est simple et intuitive, comme vous pouvez le voir sur la Fig. 4.



Dans la partie centrale de la fenêtre, très similaire à celle de l'Explorateur de Ressources de l'ordinateur, vous trouverez la liste des actions possibles concernant le Log, à savoir l'utilisation de l'ordinateur par certaines personnes. N'oubliez pas en effet que ce programme permet de garder une trace de toutes les activités exécutées au travers du clavier, en enregistrant des caractères de langage spécifiques, ainsi que la date et l'heure relevés par le système d'exploitation. Le menu vertical de la partie gauche de la fenêtre contient une série d'icônes : cliquez par exemple sur la première, Users, et le sous-menu indiquera que vous êtes actuellement le seul connecté au système. Cliquez, dans votre cas, sur Roberto, et la fenêtre principale affichera la liste de toutes les touches tapées précédemment sur le PC – même

celles relatives à différentes applications – mais aussi le texte tapé pour ce tutorial, comme montré à la Fig. 5.



■ AUTRES FONCTIONNALITÉS

En cliquant sur l'icône refresh, située dans la barre du menu horizontale, dans la partie supérieure de la fenêtre, le système actualisera les dernières opérations effectuées. Nous vous conseillons de vous familiariser avec les icônes du menu vertical sur la gauche, qui donnent accès à des fonctions de contrôle plus spécifiques qui, cela dit, ne sont pas toutes disponibles dans la version gratuite du software. Vous pouvez ainsi vérifier le contenu des chats lancés sur les différents systèmes de messagerie instantanée, afficher les fenêtres des sites web visités récemment, les applications utilisées ou paramétrer un intervalle de temps où effectuer des captures d'écran, comme reporté à la Figure 6.



Les fonctionnalités de KGB Free Keylogger s'avèrent donc indispensables pour les ordinateurs installés dans des zones dites "à risque", que ce soit à la maison ou au bureau, non seulement pour contrôler les activités des autres utilisateurs, mais aussi pour sauvegarder des travaux qui pourraient être perdus en cas de bug. Seule limite de la version gratuite du programme : l'impossibilité de l'activer automatiquement et de façon invisible au démarrage du système d'exploitation. Un problème qui peut malgré tout être résolu en téléchargeant une version ultérieure.

FIREWALL, UN MUR INFRANCHISSABLE ?

Pour naviguer en toute sécurité sur Internet sans prêter garde aux joyeux lurons qui en profitent pour s'infiltrer dans votre ordinateur, vous n'avez d'autre choix que d'installer un bon pare-feu.

Nombreux sont ceux qui pensent résoudre le problème de la sécurité en n'installant qu'un antivirus. Mais en réalité, ce dernier ne s'occupe pas des intrusions d'inconnus ni même de bloquer d'éventuels programmes instables pour votre PC, en provenance de l'extérieur. Lorsque vous naviguez sur Internet, vous n'êtes pas sans savoir que vous laissez des traces et ce, pour

le plus grand bonheur de ceux qui souhaitent

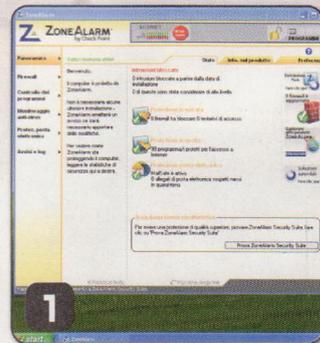
espionner vos données sensibles, en parvenant même à s'infiltrer dans les librairies système. Vos habitudes peuvent être ainsi étudiées. Et vous risquez même d'être victime de certaines fraudes informatiques surtout si vous êtes habitué à acheter online ou à surfer souvent sur le Net. Pour faire face à ce genre de désagrément, vous devez installer un pare-feu, un programme qui se charge de votre connexion et des données qui sortent de votre PC ou y entrent. Parmi ces derniers :

Zone Alarm, un logiciel gratuit développé par Zone Labs. Mettons fin dès maintenant aux idées reçues : un programme freeware n'est pas signe d'instabilité ou d'absence de maturité. En effet, Zone Alarm a été réalisé pour garantir une sécurité totale. D'ailleurs, il est tellement efficace qu'il en est parfois agaçant. Objectifs de ce programme ? Gérer les autorisations des logiciels utilisés par l'ordinateur tandis que vous naviguez, ou vice versa, contrôler et vous alerter de toute tentative d'intrusion.

1 TÉLÉCHARGEZ ET INSTALLEZ ZONE ALARM

Vous pouvez télécharger gratuitement ce software sur le site www.zonealarm.com.

Mais attention, car le site propose également des versions payantes. Pour mieux vous orienter, sélectionnez donc la rubrique protection par firewall, sous la section Protégez-vous. Une fois la nouvelle page ouverte, sélectionnez la rubrique Zone Alarm, dans le menu de gauche, et téléchargez-le. Pour l'installation, suivez la procédure guidée.



2 CONFIGUREZ ZONE ALARM

Une fois l'installation achevée, un tutoriel apparaîtra dès le premier lancement de Zone Alarm pour vous fournir une brève explication quant au fonctionnement du programme. Dans la fenêtre principale, paramétrez Zone Alarm pour qu'il vous avertisse ou non de toute tentative d'intrusion, même celles



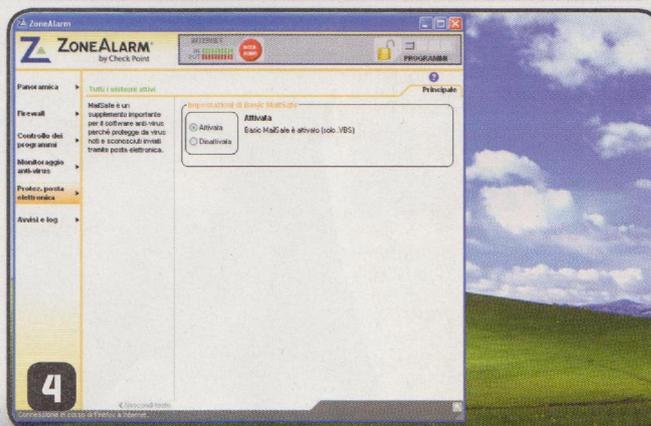
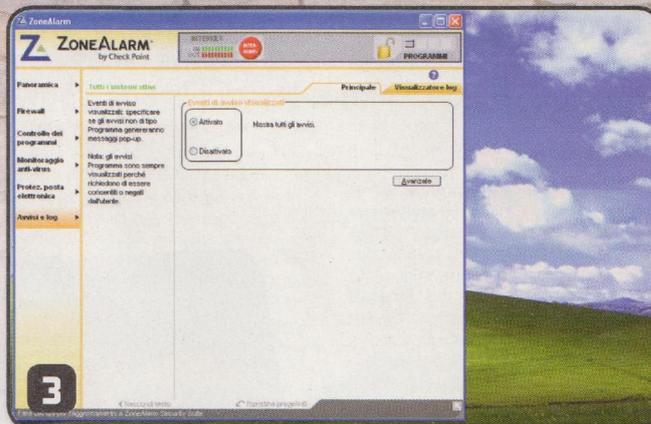
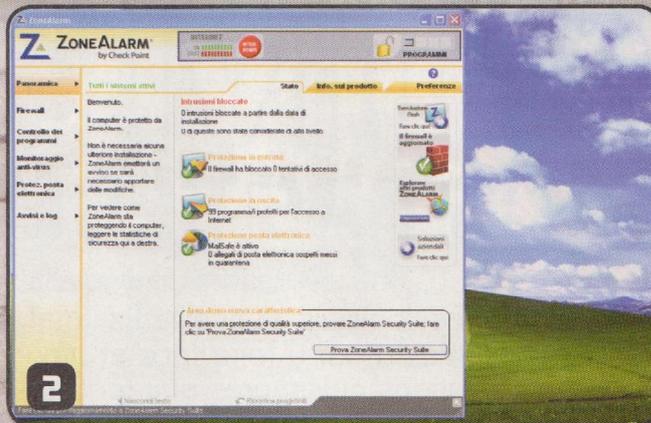
légitimes, venant par exemple de sites bancaires exigeant des codes confidentiels : supprimer ce paramètre ne signifie pas pour autant que le programme cessera de fonctionner. Il vous avertira uniquement des intrusions les plus dangereuses, et continuera d'exercer son contrôle en arrière plan, même sur le trafic interne. Pour désactiver ce paramètre, entrez dans la section Alertes et Historiques et cochez l'option Désactivé sur Alertes présentées.

3 PROTÉGEZ VOS MAILS

Autre section à configurer sur-le-champ : Basic MailSafe. Sa fonction consiste à filtrer les pièces jointes de vos e-mails et à supprimer celles potentiellement dangereuses pour votre ordinateur. Malheureusement dans la version gratuite, cette fonction est limitée et ne bloquera qu'un certain type de pièces jointes : celles portant l'extension .VBS. Associé au contrôle de votre antivirus, il vous permettra toutefois de dormir tranquille. Pour activer cette fonction, il vous suffira de cocher tout simplement Activé.

4 PARAMÉTRER LES AUTORISATIONS DE VOS PROGRAMMES

Une fois Zone Alarm activé, tout programme dorénavant ouvert sera bloqué et contrôlé immédiatement. Comme vous pouvez l'imaginer, ces alertes pourraient bien vite devenir agaçantes, surtout si vous connaissez bien le programme que vous ouvrez. Armez-vous donc de patience et au fur et à mesure que vous ouvrez vos programmes, configurez Zone Alarm de sorte qu'il les reconnaisse immédiatement sans bloquer la procédure d'ouverture. En effet, une alerte apparaîtra en bas à droite pour vous demander si vous souhaitez ou non autoriser le programme lancé. Si vous optez pour la première solution, n'oubliez pas de sélectionner l'option Conserver ce paramètre de façon à rendre votre choix définitif.



FIREWALL

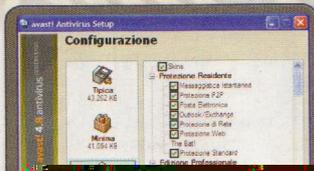
ANTIVIRUS... MAIS PAS SEULEMENT !

Aujourd'hui, les logiciels malveillants (malwares) sont de plus en plus sophistiqués. Pour y faire face et protéger votre ordinateur, de nouvelles solutions puissantes aux fonctionnalités innovantes vous sont proposées. Leur fiabilité est incontestable puisqu'elles peuvent affronter les formes d'attaque les plus diverses en provenance de l'extérieur. Avast! est l'une d'entre elles. Un antivirus qui, dans sa dernière version, intègre des outils anti-spyware et anti-rootkit.

Quand on songe aux premiers virus qui, dans la seconde moitié des années 80, se manifestaient sur les ordinateurs infectés en créant des boules qui rebondissaient d'un côté à l'autre de l'écran ou des fenêtres qui disparaissaient subitement devant les yeux atterrés des utilisateurs, il y a aujourd'hui de quoi sourire ! Mais la menace des nouveaux malwares est un problème bien plus sérieux ! Comme vous le savez déjà, la lutte contre ces pièges passe tout d'abord par l'installation d'un logiciel antivirus, à même de prévenir les nombreuses formes d'attaque et de restaurer l'intégrité d'un système éventuellement corrompu par le malware. Parmi les solutions gratuites les plus efficaces, notons Avast! Antivirus, de la société tchèque ALWIL Software qui, dans sa toute dernière version 4.8, intègre des fonctionnalités anti-spyware et anti-rootkit renforcées. Vous pouvez télécharger ce programme sur le site www.avast.com : en vous connectant à la page d'accueil, comme montré Fig. 1, vous pouvez accéder aux zones qui vous intéressent à travers la barre horizontale du menu, placée



dans la partie supérieure. Rappelons qu'Avast Home Edition, à savoir la version gratuite du software, ne peut être utilisé que par des particuliers : l'utiliser en entreprise et à des fins commerciales est donc tout à fait illicite.



à la fenêtre qui vous permettra d'agir sur chaque application contrôlée par l'antivirus, comme vous pouvez le voir Fig. 4.



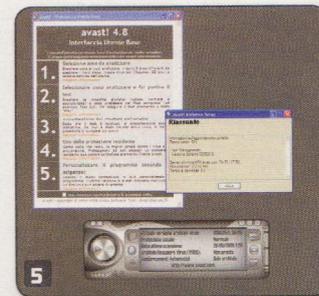
1 ■ TÉLÉCHARGEZ ET INSTALLEZ LE PROGRAMME

Dans l'espace de téléchargement, après avoir sélectionné Avast! 4 Home Edition dans la liste des produits en fonction du système d'exploitation utilisé, vous serez redirigé vers une autre page, où vous pourrez choisir la langue d'installation du programme. Il vous faudra ensuite télécharger le fichier Setup. exe, après avoir choisi sa destination d'enregistrement. Une fois le fichier téléchargé, vous pourrez lancer la procédure de setup en suivant les indications des différentes fenêtres. Vous devrez surtout prêter attention à la fenêtre relative à la configuration du programme, qui vous permettra de choisir votre mode d'installation : typique, minimale ou personnalisée. Selon l'option sélectionnée, le menu déroulant vertical sur la droite vous indiquera les fonctionnalités correspondantes. En cas d'installation personnalisée, vous pourrez paramétrer ces fonctionnalités en cochant ou décochant les cases correspondantes, comme montré Fig. 2.

vous demandera si vous souhaitez effectuer un contrôle antivirus des disques durs lors du prochain redémarrage de l'ordinateur. Bien sûr, c'est l'occasion ou jamais de mettre à l'épreuve Avast! 4. Redémarrez donc votre ordinateur pour vérifier l'intégrité du système et permettre au programme d'achever son installation. Le scan précède le boot de Windows, et peut prendre quelques dizaines de minutes, selon la quantité de fichiers présents dans l'ordinateur. Si des logiciels malveillants sont présents dans le système, Avast! vous avertit alors immédiatement et active la procédure pour restaurer ou supprimer les fichiers corrompus. Dans le cas contraire, si l'ensemble du système est clean, vous pouvez procéder à la configuration. Dans la barre des tâches du système d'exploitation, deux nouvelles icônes sont apparues : deux petites boules bleues portant les lettres i et a, comme montré Fig. 3.

La première représente le générateur de la base de récupération VRDB qui, en travaillant en arrière-plan, acquiert des informations sur les programmes et, en cas d'infection, aide Avast! à bien supprimer le virus. En double-cliquant sur la petite boule a, vous ouvrirez la fenêtre qui reporte l'état de l'antivirus avec les informations sur le niveau de protection résidente, que vous pourrez paramétrer selon vos exigences de normale à élevée, sans oublier la liste des processus soumis au contrôle. En cliquant sur le bouton détails, vous accéderez

A présent, lancez le programme à partir de l'icône principale. Une fois le scan de la mémoire effectué par l'antivirus, l'interface utilisateur s'activera, semblable à celle d'un lecteur audio, outre une fenêtre expliquant en cinq points la façon d'utiliser les commandes. En cochant la case en bas à gauche, cette fenêtre d'assistance ne s'affichera plus lors des démarrages suivants. Cette interface vous permettra non seulement d'afficher l'état général de l'antivirus et ses activités, mais aussi de mettre à jour la base de données virale à travers sa commande manuelle. Cliquez sur cette dernière pour récupérer et télécharger les fichiers les plus récents à partir du serveur d'Avast!, comme montré Fig. 5.



N'oubliez pas qu'une solution antivirus, toute aussi puissante et fiable soit-elle, est inutile si elle n'est pas régulièrement mise à jour. Vous devez donc prêter une attention toute particulière aux fonctionnalités du logiciel et à leurs paramètres, en vous familiarisant avec les commandes de mise à jour manuelle et les options proposées par le fabricant.

IRUS

AVEC LOGMEIN, VOTRE ORDINATEUR VOUS SUIT PARTOUT !

Se connecter à son bureau, partout dans le monde et gratuitement, c'est aujourd'hui possible, grâce à LogMeIn ! Un logiciel d'accès à distance basé sur une interface web côté client, qui permet de contrôler jusqu'à trois ordinateurs.

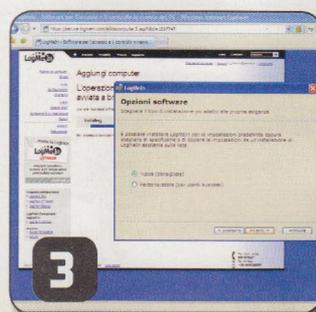
Un ami dans une autre ville qui a besoin d'aide pour résoudre un problème sur son PC ? Une maman peu branchée technique qui ne parvient pas à configurer sa webcam ? Ou, tout simplement, la nécessité d'utiliser son PC perso ou pro lorsqu'on ne l'a pas sous la main ? LogMeIn est la solution qu'il vous faut, simple et surtout gratuite. Développé par la société américaine du même nom, ce logiciel est en effet basé sur une interface web côté client, et permet d'accéder aux ordinateurs enregistrés à partir de tout autre terminal connecté au Net et équipé d'un

navigateur. LogMeIn est également disponible en version gratuite, une version qui vous permettra de contrôler jusqu'à trois ordinateurs différents. Les plus exigeants pourront quant à eux opter pour la version Pro, commercialisée à un prix proportionnel au nombre de machines à enregistrer : à titre d'exemple, 235,00 € pour cinq ordinateurs. Quant aux autres fonctionnalités de LogMeIn Pro, elles vous permettront de transférer des fichiers vers d'autres ordinateurs, d'inviter d'autres utilisateurs à visualiser votre propre bureau ou de leur envoyer un lien via Ftp vers les fichiers de votre PC.

Pour télécharger ce logiciel, vous devez tout d'abord vous enregistrer, en vous connectant à la page www.logmein.com, comme montré Fig. 1.

■ PROCÉDURE D'ENREGISTREMENT

La page d'accueil vous permettra d'accéder à toutes les informations sur les services proposés aux utilisateurs, en cliquant par exemple sur les différentes zones de la partie centrale : Support informatique et assistance à distance, Accès à distance, RPV



instantané et Sauvegarde. Pour afficher la liste complète des produits ou les tarifs correspondants, déplacez-vous en revanche parmi les rubriques de la barre horizontale du menu, placée dans la partie supérieure de la page. En bas, deux liens vous orienteront vers l'assistance pour déterminer le produit le plus adapté à vos exigences et à la création d'un compte personnel, une phase toutefois intégrée à la procédure d'installation du software qui s'active en cliquant sur le bouton de téléchargement de LogMeln Free, situé au milieu de la page. Un numéro vert d'assistance téléphonique est en outre disponible : 800-873217. Première étape de la procédure guidée d'installation, à la fois simple et intuitive : vous créer un compte pour pouvoir enregistrer l'ordinateur souhaité au service. En cliquant sur le bouton de téléchargement, vous serez redirigé vers la fenêtre d'inscription, où vous devrez indiquer un e-mail et un mot de passe personnel, comme le montre la Fig. 2.

■ TÉLÉCHARGEMENT ET INSTALLATION

Après avoir confirmé vos données, vous passerez à la page Ajouter un ordinateur, qui vous affichera l'état de progression du téléchargement du software. Dans la boîte mail indiquée précédemment, vous trouverez deux messages : un de bienvenue avec un guide général sur les fonctionnalités du service, et un autre proposant un lien sur lequel vous devrez cliquer pour confirmer l'activation de votre compte. A la fin du

téléchargement, la procédure d'installation se lance. Suivez donc les indications des fenêtres pour l'acceptation du contrat de licence et la configuration du programme avec le nom de l'ordinateur et le type d'installation, typique ou personnalisée, comme montré Fig.3.

A la fin de la procédure, le système vous demandera d'installer un composant Active-X. Les paramètres de sécurité du système d'exploitation utilisé peuvent automatiquement demander l'accord de l'utilisateur en présence de fichiers et programmes "inconnus". Dans le cas présent, vous pouvez procéder sans problèmes à l'installation d'Active-X qui, une fois achevée, laissera place à la fenêtre de confirmation d'enregistrement de votre ordinateur. Sur la partie droite de la page, vous trouverez la commande qui vous permettra d'ajouter d'autres terminaux, tandis que la barre horizontale au centre affichera l'état de l'ordinateur utilisé, comme indiqué à la Fig. 4

■ CONTRÔLE À DISTANCE

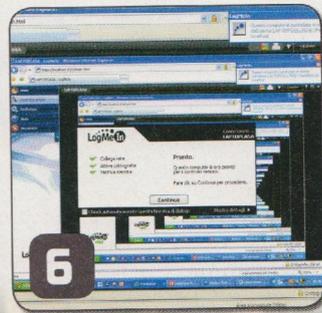
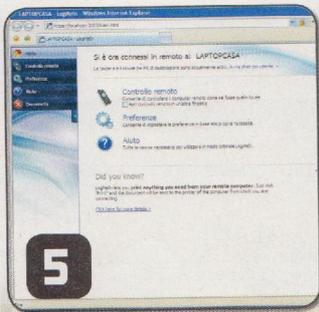
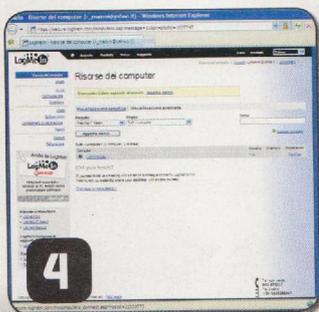
Vous êtes donc prêt à agir loin de votre ordinateur qui, bien sûr, doit être lui aussi connecté à Internet. Si vous y accédez depuis un autre PC, en vous connectant à LogMeln et en accédant à votre compte, la page décrite précédemment s'affichera. En cliquant sur le nom de l'ordinateur enregistré, que nous avons appelé dans le cas présent Laptopcasa, le navigateur affichera une page de confirmation de

la connexion à distance en cours avec votre bureau. Vous pouvez régler d'autres paramètres de configuration selon vos exigences, en sélectionnant la rubrique Contrôle à distance, qui peut également s'afficher dans une autre fenêtre, ou celle des Préférences, comme le montre la Fig. 5.

Dans la section Aide, vous trouverez toutes les ressources nécessaires pour une utilisation optimale de LogMeln, tandis qu'en cliquant sur la commande placée dans la partie supérieure, vous pourrez lancer un chat avec l'utilisateur de l'ordinateur distant. Le bureau de ce PC peut être facilement commandé à travers la souris et le clavier.

■ UN TEST AMUSANT

Si, après avoir effectué l'installation de LogMeln sur l'ordinateur, vous vous arrêtez sur la page de confirmation de l'enregistrement de la Fig. 4, vous pouvez cliquer sur le nom du PC enregistré, donc celui-là même sur lequel vous êtes en train de travailler. Une fenêtre apparaîtra où le système vous fera gentiment remarquer qu'il ne semble pas très logique de se connecter via Internet, avec LogMeln, à votre propre ordinateur. Dans tous les cas, en devinant votre curiosité... il vous demandera si vous souhaitez forcer la procédure de connexion. Quelle question ! Bien sûr ! Confirmez, et votre bureau apparaîtra sur l'écran répliqué à l'infini, comme montré Fig.6.



ANTI-ROOTKIT

Un rootkit est un programme exploité pour masquer la présence d'un objet ou d'un processus à l'utilisateur ou l'administrateur de l'ordinateur.

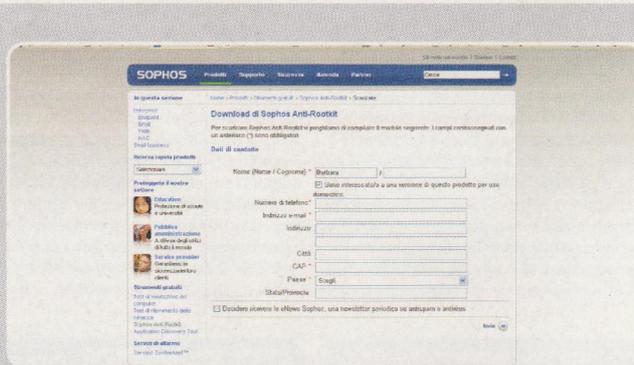
Ces programmes sont conçus de façon à tromper les contrôles de sécurité des systèmes d'exploitation. Se rendre compte de leur présence n'est pas chose facile. Les rootkit sont souvent utilisés pour cacher des backdoor, à savoir des «accés alternatifs» à votre ordinateur qui permettent de contourner ses systèmes de sécurité. Mais les pirates utilisent aussi les rootkit pour

compliquer la détection de chevaux de Troie et autres spywares spécifiques, en masquant leurs processus principaux. Ils peuvent aussi être exploités pour trouver et soustraire des informations personnelles présentes dans votre ordinateur. Alors, comment

se défendre face à un ennemi aussi insidieux ? Tout simplement en s'appuyant sur un programme spécialisé, tel qu'Anti-Rootkit.



TUTORIAL



LE CD FOURNI AVEC LA REVUE CONTIENT UNE VERSION DU PROGRAMME mais n'hésitez pas à vous connecter au site de Sophos (<http://www.sophos.fr/products/free-tools/sophos-anti-rootkit.html>), vous y trouverez les toutes dernières versions à télécharger (le programme ne prévoit pas de mise à jour automatique). Pour cela, vous allez devoir remplir un formulaire obligatoire, mais la procédure est rapide.

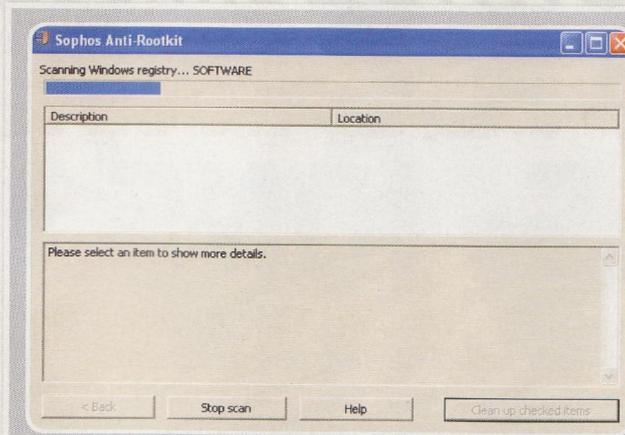
Sophos Anti-Rootkit setup



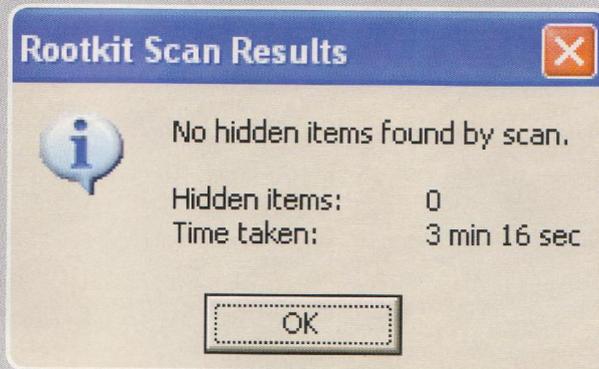
Sophos Anti-Rootkit was successfully installed. Click 'yes' to start it now.

Si No

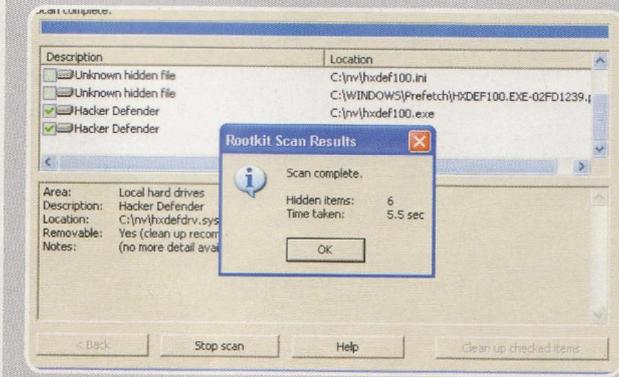
L'INSTALLATION EN ELLE-MÊME EST TRÈS SIMPLE. Double-cliquez sur le fichier sarsfx.exe et acceptez le contrat de licence d'utilisation, en cliquant sur Accept. Quelques secondes plus tard, un message vous demandera de cliquer sur 'Oui' pour lancer le programme.



A PRÉSENT, VOUS ALLEZ VOIR APPARAÎTRE UNE FENÊTRE QUI DOIT VOUS PERMETTRE D'ANALYSER VOTRE ORDINATEUR pour trouver et supprimer les rootkit éventuellement présents. Vous pouvez décider de faire une analyse complète sans toucher aux trois options : Running processes (processus en cours), Windows registry (registre Windows) et Local hard drives (disques durs locaux), ou bien paramétrer une analyse plus spécifique, en décochant les options qui ne vous intéressent pas. Vous pourrez toujours les re-sélectionner par la suite. Vous pouvez de nouveau lancer le programme à partir du menu Démarrer, Programmes/Sophos/Sophos Anti-rootkit.



CHOISISSEZ L'ANALYSE COMPLÈTE ET CLIQUEZ SUR START SCAN. Si, pour une raison ou pour une autre, vous voulez interrompre l'opération, il suffit de cliquer sur Stop scan. Une fois l'analyse terminée, une fenêtre de dialogue s'ouvrira pour vous informer des résultats obtenus. Si tout va bien, vous devriez trouver une fenêtre comme celle-ci.



SI EN REVANCHE VOUS TROUVEZ DES ÉLÉMENTS CACHÉS, le programme vous les signalera. La partie basse de la fenêtre indique leur classification. Si vous voyez inscrit le message Removable : No, cela signifie qu'il est impossible de les supprimer. Si en revanche vous voyez apparaître Removable : Yes (clean up recommended), il est alors conseillé de les supprimer en cliquant sur Clean up checked items après les avoir cochés. Si vous trouvez l'indication Removable : Yes (but clean up not recommended for this file), cela signifie que le programme ne les reconnaît pas et que leur suppression ne serait pas très prudente. Vous pouvez toutefois les signaler au développeur en allant directement sur son site. Une fois cette procédure terminée, redémarrez l'ordinateur et faites une analyse antivirus car la suppression des rootkit pourrait révéler la présence de malwares.

TRAQUEZ LES ESPIONS !

Parfois, nos informations confidentielles ne sont pas directement menacées par Internet, mais par des attaques qui, elles, n'ont rien de virtuel ! Heureusement, des solutions existent. Voici donc quelques conseils pour mettre sur pied un véritable système de défense et de contrôle. Il ne vous en coûtera que quelques euros et quelques notions d'électronique.

Vos informations confidentielles font l'objet de nombreuses attaques, dont la plupart proviennent de simples programmes qui tentent de s'introduire dans votre ordinateur, dans un objectif bien précis. Comme tout le monde le sait, bon nombre de ces menaces sont plus gênantes qu'autre chose. Or, il existe un type d'intrusion qui, lui, présente un réel danger : l'intrusion physique dans notre vie privée, comme lorsque quelqu'un profite de votre absence pour fouiner dans vos affaires en toute impunité. Des voyeurs qui peuvent envahir votre poste de travail, votre bureau ou encore n'importe quelle autre pièce commune. Alors passez dès maintenant à l'offensive ! Vous pouvez pour cela utiliser toute une série de contremesures, dont la plupart sont totalement gratuites ou presque.

■ UN PEU DE THÉORIE

Les experts en sécurité savent qu'un système inviolable relève du pur fantasme. Toute protection, quelle qu'elle soit, peut être violée d'une façon ou d'une autre, qu'il s'agisse de la chambre forte d'une banque

ou d'un pare-feu. L'important, c'est donc que ces protections tiennent suffisamment longtemps pour démotiver l'agresseur. L'objectif que nous nous fixons ici est de mettre sur pied un système capable de décourager les curieux ou du moins de les garder à l'œil. Un système qui n'aurait sans doute aucune efficacité contre des professionnels ou des petits malins, mais qui se révèle plus que suffisant pour les fouineurs basiques, ceux qui ont toujours besoin de toucher à tout. Avant de commencer, vous devez définir vos priorités. En première analyse, il vous faut établir deux catégories de contremesures : "actives" et "passives". Les premières visent à décourager directement ceux qui s'approchent d'un peu trop près à vos affaires, bref, à les empêcher de vous espionner. Une catégorie qui englobe les panneaux d'interdiction d'accès, les portes, mais aussi différents types d'alarmes. Les formes de défense dites "passives" vous permettent quant à elles de surveiller votre environnement même lorsque vous n'êtes pas chez vous. Elles comprennent les caméras vidéo, micros et tous les outils qui vous permettent d'observer une zone à distance.

■ DÉFENSE MAISON

Dans la mesure où les systèmes de défense actifs sont plutôt contraignants à mettre en place en open space, il ne vous reste plus qu'à vous replier sur les systèmes passifs. Ces derniers offrent un avantage incontestable : s'il est indéniable qu'ils n'interrompent pas l'action du curieux, ils vous permettront néanmoins d'observer celui ou celle qui vous espionne et de le prendre en flagrant délit. Outre votre ordinateur, tout ce dont vous avez besoin pour mettre en place une bonne défense, c'est d'une bonne vieille webcam et d'un téléphone portable inutilisé. Bien sûr, ces deux périphériques doivent être en bon état de fonctionnement. Nous verrons dans les pages suivantes comment les transformer en véritables outils d'espionnage. L'idée de base consiste à construire un petit système de contrôle audio et vidéo en exploitant votre ordinateur et Internet comme système de transmission pour recevoir les images de la webcam, où que l'on soit. Vous devez avant tout transformer votre webcam en système infrarouges, grâce à une petite astuce et en exploitant les avantages des capteurs CCD que toute webcam contient.

WEBCAM INFRAROUGE



1 Procurez-vous une vieille webcam et essayez de l'ouvrir. En fonction des modèles, il suffit parfois de dévisser la lentille ou encore d'ouvrir le boîtier. Dans ce cas, voyez un peu s'il y a des vis à retirer ou s'il suffit de désencaster le boîtier.



2 Le capteur est généralement protégé par une petite protection sur laquelle est vissée la lentille. Retirez les deux composants ou tentez de nouveau de dévisser la griffe pour la mise au point.



3 Le filtre est un petit verre. Même si, à première vue, il semble transparent, en l'observant à contre-jour ou en le photographiant, vous le verrez légèrement rouge. C'est celui que vous devez remplacer pour changer le spectre de la webcam.



4 Choisissez une zone totalement noire d'un vieux négatif et coupez quelques morceaux de la même forme que le filtre. Plus sombre est la zone, et mieux ce sera. On trouve généralement en début de pellicule un bout totalement noir, qui fera parfaitement l'affaire ici.



5 Installez le "nouveau" filtre à sa place. Certains modèles disposent d'un système d'emboîtement. Pour les autres, vous allez devoir utiliser un peu de colle. Dans ce cas, nous utiliserons une aiguille ou un cure-dents pour un travail plus précis.



6 Refermez la webcam en faisant bien attention à la disposition des pièces. Les fils de connexion sont plutôt fragiles, veillez à les positionner correctement de façon à ce qu'ils ne s'abiment pas.

SOLUTIONS DANS LE COMMERCE

Si vous ne vous sentez pas le courage de démonter une vieille webcam pour créer votre système de surveillance infrarouge, vous pouvez toujours en acheter une dans le commerce. La Slim 311R de Genius, www.geniusnet.com est déjà équipée d'un système infrarouge et dispose des LEDS nécessaires pour éclairer une pièce en toute discrétion.

■ LE TRUC EN QUESTION

Comment obtient-on un résultat aussi efficace avec un truc aussi simple ? Tout simplement grâce aux différentes longueurs d'onde de la lumière. Concrètement, notre œil capte uniquement une petite partie des ondes électromagnétiques émises par les objets, à savoir la lumière visible. Les capteurs CCD des webcams sont quant à eux capables d'en recevoir une partie bien plus large. Pour que les images perçues par la webcam soient cohérentes avec celles que vous voyez, les fabricants appliquent un filtre qui "coupe" les émissions hors du spectre. En d'autres termes, le verre que vous avez retiré a pour mission de supprimer les émissions invisibles à l'œil humain. Les parties sombres de la pellicule photo, en revanche, isolent presque totalement la lumière visible, c'est pourquoi elles apparaissent pratiquement noires à l'œil, mais se révèlent quasi transparentes en vision infrarouge. En les utilisant comme filtres, le capteur recevra et transmettra la lumière infrarouge au lieu de celle que nous voyons normalement. L'acquisition des images effectuée par l'ordinateur fera le reste.

■ UTILISATION DES IMAGES

Travailler sur le côté "mécanique" de la webcam présente un avantage incontestable. Vous pouvez en effet conserver toute la partie software que vous utilisez normalement. Le système d'exploitation ne perçoit aucune différence, si ce n'est dans le calibrage que vous allez probablement devoir revoir dans la mesure où la sensibilité du récepteur a probablement changé après la modification. Pour le reste, c'est toujours pareil. Certes, vu que les images sont affichées en noir et blanc et que les couleurs ne correspondent pas à celles que l'on voit habituellement, votre webcam ne sera plus l'idéal pour les programmes de chat. Vous pourrez toutefois l'utiliser pour effectuer un contrôle distant, même en conditions de lumière peu favorables, là où les webcams traditionnelles trouvent leur limite. Vous pouvez par exemple utiliser l'un des



Une alarme de porte et un peu de ruban bi-adhésif peuvent transformer une simple porte en porte de sécurité. Il suffit d'installer l'alarme dans un lieu peu visible et de compter sur l'effet de surprise.

nombreux programmes de détection de mouvement pour transmettre ensuite des images vers une adresse e-mail, ou publier le flux de données sur une page web pour qu'il soit toujours accessible. Certains programmes de vidéosurveillance sont généralement inclus dans le pack d'installation de la webcam, même si Internet en propose un grand nombre. Vous pouvez jeter un coup d'œil sur LiveStream, <http://live-stream.net> ou encore sur SecureCam, <http://www.brooksyounce.com/soft/securecam.htm>.

■ AMÉLIORER LE RENDU

Si vous avez un téléphone portable capable de se connecter à Internet, il suffit de charger les

images sur une page web ou de les envoyer vers une adresse e-mail que vous pouvez contrôler depuis votre mobile, pour garder votre espace sous contrôle en deux temps trois mouvements. Dernier problème : l'éclairage. En effet, votre webcam infrarouge réagit aussi bien à la lumière normale qu'à celle provenant de basses fréquences. Essayez par exemple d'éteindre la lumière et "d'éclairer" quelque chose en utilisant une télécommande pour voir votre dispositif en action. Pour disposer d'un éclairage plus homogène, vous pouvez vous procurer des LEDS infrarouges chez un revendeur en électronique et les alimenter tout simplement avec des piles alcalines. Vous pouvez aussi acheter une lampe-torche à LEDS et remplacer celles connectées par les nouvelles. Ainsi, la lumière ne sera pas visible à l'œil nu mais vous permettra de filmer sans que personne ne s'en aperçoive.



Une caméra avec un jeu de lumières intégrées

LE TÉLÉPHONE ESPION



1 Procurez-vous un vieux téléphone et commencez par sa configuration. Paramétrez la réponse automatique à partir du menu, éteignez-le, retirez la batterie et assurez-vous que les paramètres soient bien gardés en mémoire. Puis ouvrez-le et retirez batterie et carte SIM



2 Les portables sont plutôt durs à ouvrir. Aidez-vous du manuel et des conseils prodigués sur Internet. Retirez ensuite soigneusement toutes les parties mobiles que vous trouverez



3 Souvent, les portables utilisent des vis de type Torx. Vous trouverez les tournevis correspondants chez les revendeurs d'électronique ou d'électrotechnique. En cas de doutes, apportez avec vous la coque et faites des tests avant d'acheter ce dont vous avez besoin



4 Le retrait du haut-parleur peut parfois s'avérer quelque peu laborieux. Sur certains modèles, il est juste enclenché. Sur d'autres en revanche, vous aurez peut-être besoin de pincettes ou d'un petit poste de soudure. Gardez-le ensuite sous la main.



5 Pour éviter que le téléphone ne s'allume en cas d'appel, le plus simple reste encore de couvrir l'écran et les éventuelles LEDS. Facile à retirer, le ruban adhésif américain ou un ruban adhésif isolant ordinaire fera parfaitement l'affaire.



6 Une fois ces opérations terminées, refermez le téléphone, allumez-le et faites un test. N'oubliez pas que votre portable est à présent totalement privé de son. Tout fonctionne normalement ? Alors préparez l'endroit où le cacher !

LA CACHETTE IDÉALE

Vous n'arrivez pas à vous décider pour trouver une bonne cachette pour votre téléphone ? Voici venu le moment de vous connecter à Internet. Les livres creux sont une excellente idée pour y cacher des objets. Allez trouver l'inspiration sur www.booksafes.co.uk. Si sacrifier l'encyclopédie que vous a offerte votre grand-mère pour votre communion n'est peut-être pas la meilleure idée, optez plutôt pour un livre bon marché ou une vieille BD !

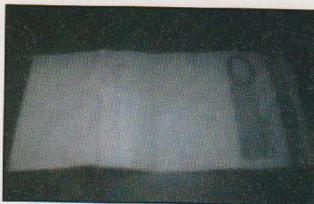


■ TOUT EST PRÊT ?

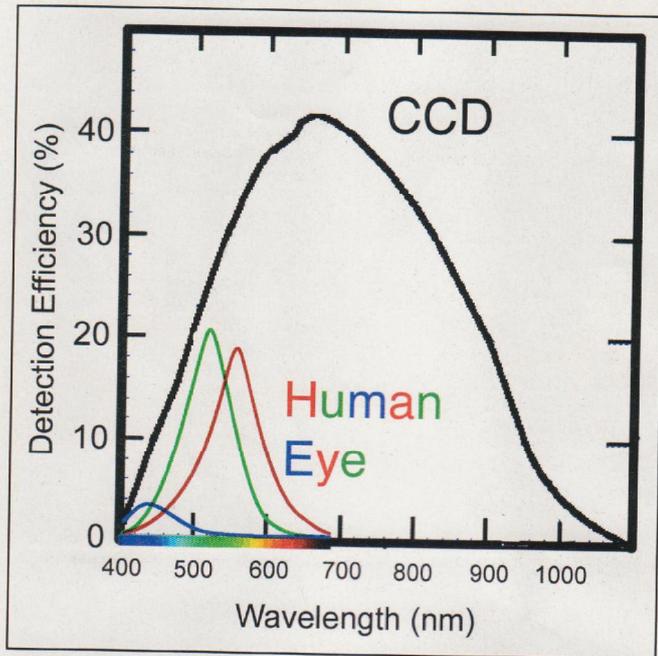
Une fois votre vieux portable bien dissimulé, vous êtes maintenant prêt à l'utiliser comme système d'écoute. N'oubliez pas d'installer à l'intérieur une carte SIM pour qu'il reste joignable. L'idéal étant de l'utiliser combiné à la webcam pour éviter d'avoir à passer des appels aléatoires pour tenter de découvrir quelque chose. Dès que vous recevez un mail, vous pouvez passer un appel et écouter tout ce qui se passe. Si ça marche, essayez de placer le mobile dans une zone facilement accessible mais bien dissimulée, par exemple dans un placard ou sur une étagère. Dans la mesure où certaines des opérations que vous faites subir à votre portable pour le transformer en système espion sont irréversibles, il convient de procéder à quelques tests avant de l'ouvrir et de le modifier, surtout concernant l'écran. C'est pourquoi mieux vaut appliquer une protection amovible, comme du ruban adhésif américain. Ainsi, en cas de panne, vous pourrez de nouveau avoir accès à l'écran et contrôler ce qui ne va pas.

■ PLEINE CHARGE !

Le seul problème du système que vous avez mis en place concerne la durée des batteries. Si vous avez recyclé un vieux téléphone, sa batterie ne devrait pas battre des records d'autonomie et risque de vous planter en plein milieu d'une écoute ! Pour limiter les coûts, inutile de vider votre portefeuille dans l'achat d'une



Voici comment se présente un vrai billet passé à l'infrarouge. Les encres sont étalées de façon à réfléchir la lumière par zones. Un simple passage suffit pour déceler les faux billets



Les différents spectres de détection des différentes couleurs par l'œil humain et par une camera (CCD).

nouvelle batterie. Si vous voyez que le système fonctionne, le plus important est de trouver la façon dont le garder constamment en charge. Pour cela, vous pouvez tout simplement cacher le câble en priant pour que personne ne se demande où il mène en voyant la prise, ou encore vous procurer un chargeur de batterie USB et le brancher au PC. Les câbles qui partent d'un ordinateur sont moins "suspects" que ceux reliés à une prise électrique et ont donc plus de chance de passer inaperçus. Vous trouverez ce type de câble dans les magasins d'électronique ou chez votre revendeur online. Certes, la batterie d'un téléphone portable branché en permanence ne risque pas de faire long feu, mais ce n'est pas ce qui nous préoccupe ici.

■ AMÉLIORER LA PRISE

Positionner un téléphone portable

de façon à ce qu'il soit bien caché tout en captant bien le son n'est pas chose aisée. La portée des micros des portables est en effet plutôt limitée et les bruits de fond risquent de couvrir les conversations. Une fois encore, la solution se trouve dans le commerce. Il suffit d'utiliser un écouteur filaire pour résoudre ce dernier problème. L'avantage de ce type de système ? La possibilité de mieux dissimuler le téléphone pour s'occuper uniquement de l'écouteur, plus facile à cacher. Certes, cela requiert quelques efforts, mais vous allez bientôt pouvoir garder sous contrôle votre espace privé sans que personne ne s'en aperçoive. Evitez les lieux trop visibles ou ceux où dans lesquels les objets sont souvent utilisés. Il serait dommage que la première personne venue tombe sur votre système en allant chercher un simple livre !



Vue aux infrarouges, une simple télécommande se transforme en une sorte de torche électrique. Si vous essayez, vous remarquerez qu'elle clignote. Cela correspond en fait à la séquence d'impulsions qui permet de commander la TV.

même couleur que la coque de l'appareil. Préférez la première solution : la webcam semblera ainsi éteinte. Dans le second cas, un bon observateur se rendra compte du truc. Autre possibilité, à utiliser aussi pour le téléphone : dissimuler votre kit dans différentes boîtes. Prenez par exemple une boîte à gâteaux, un livre creux ou encore le boîtier d'un dispositif quelconque, comme celui d'un vieux lecteur CD ou d'un disque dur externe. Si vous devez contrôler l'espace environnant de votre ordinateur, ces boîtiers auront peu de chance d'être soupçonnés. En outre, ils présentent l'avantage de pouvoir être branchés à une prise et au PC sans éveiller le moindre soupçon.



Les leds infrarouges peuvent augmenter la lumière lors d'une prise de vue infrarouge sans que personne ne s'en rende compte, magique !

■ TRUCS D'ESPION

Maintenant que vos systèmes de défense sont prêts et que vous avez appris quelques trucs pour les installer au mieux, voici venu le moment de parfaire le tout. La première chose à faire, c'est de trouver une cachette pour vos équipements. Pour la webcam, vous pouvez supprimer les LEDS qui témoignent de son activité. Si vous l'avez ouverte pour remplacer le filtre par le modèle infrarouge, vous pouvez en profiter pour dessouder les LEDS de la carte. Si vous n'êtes pas un pro de la soudure, vous pouvez tout simplement les recouvrir d'une couche de peinture noire ou de la

■ SOYEZ ORIGINAL !

La guerre aux espions et les contre-mesures adoptées contre la violation de nos données confidentielles ne date pas d'hier et nous enseignent une chose importante : pas besoin de se ruiner ou d'investir dans les toutes dernières technologies pour mettre en place un système efficace. Souvent, une bonne idée suffit pour prendre à contre-pied le plus grand des fouineurs, surtout s'il ne s'attend pas au piège. Les alarmes de porte que l'on trouve chez certains revendeurs de matériel électrique pour une dizaine d'euros peuvent paraître banales, mais si vous les installez à l'intérieur d'un tiroir ou sur une porte,

ils feront preuve d'une efficacité redoutable. Dans un même objectif, vous pouvez aussi recourir aux capteurs utilisés par de nombreux magasins pour signaler l'entrée des clients. En plus, pour peu que l'électronique ne vous fasse pas peur, vous pouvez supprimer leurs logements d'origine pour les occulter au mieux, ou encore utiliser les actionneurs pour faire autre chose que transmettre un son, comme par exemple allumer une radio à plein volume ou le PC. L'important, c'est de faire preuve d'originalité et de s'efforcer de penser à quelque chose de nouveau. Autres petits trucs plutôt banals mais toujours efficaces : les interrupteurs cachés pour les dispositifs électroniques. Aujourd'hui, avec les prises multiples, c'est encore plus facile ! Vous pouvez en utiliser deux en série pour vos appareils, dont une bien en vue et l'autre cachée derrière un meuble. Certes, il ne s'agit pas là d'une solution définitive, mais le fait d'avoir à chercher le second interrupteur fera perdre au curieux de précieuses secondes qui peuvent très bien le décourager d'aller plus loin.



TELEPHONE ESPION



Il ressemble en tous points à un Nokia N95 et pourtant ! Un programme spécifique permet d'écouter les appels de celui qui l'utilise, lire les Sms qu'il envoie et reçoit, jeter un œil à distance à la liste des appels reçus, des appels en absence et appels émis. Et, cerise sur le gâteau, de savoir où se trouve le malheureux qui utilise ce téléphone. Hacker Magazine a testé pour vous le plus efficace des téléphones espions...

Il y a quelques mois, la Répression des Fraudes a coincé 420 personnes qui avaient modifié leur téléphone portable de sorte qu'il puisse espionner fiancées, maris, employés et amants, en utilisant un programme spécifique. Et ce, en découvrant par la même occasion, les aventures sexuelles d'un couple vivant dans un immeuble de la banlieue de Naples : en fait, le mari était l'amant d'une femme du même immeuble. Rien d'étrange à cela me direz-vous, si ce n'est le fait que le mari de cette dernière était également l'amant de la femme trompée par le premier mari. Complicé, pas vrai ? Et c'est peu dire, puisque la Répression des Fraudes a découvert que nos quatre compères, évidemment méfiants, se contrôlaient mutuellement par le biais de télépho-



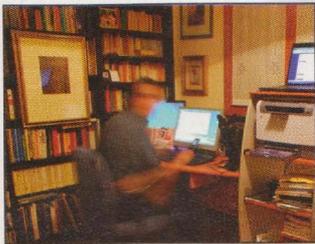
nes espions. Sans doute l'un de ceux qu'Hacker Magazine a testé pour vous. La société NeoCall nous l'a en effet gentiment envoyé. Elle les vend online sans problèmes et en toute légalité (du fait également que son siège social se trouve à Saint-Marin) à l'adresse www.neocall.it. Certes, vendre des téléphones espions depuis Saint-Marin n'a rien d'illégal ; idem pour ceux qui les achètent. En revanche, les utiliser pour contrôler des personnes à leur insu, ça c'est franchement illégal ! D'ailleurs, la loi dit textuellement à cet égard : "Quiconque prend frauduleusement connaissance d'une communication ou d'une conversation, téléphonique ou télégraphique, entre d'autres personnes ou dans tous les cas qui ne lui est pas destinée, ou encore l'interrompt ou l'empêche, est puni de 6 mois à 4 ans de réclusion". Et c'est justement ce que peuvent faire ces téléphones, peu importe leur marque et modèle, à condition de tourner sous Symbian et d'être dotés d'un software unique en matière d'espionnage téléphonique. Bien sûr si vous les achetez pour un usage licite, vous ne commettez aucun délit. Même si ce type d'utilisation est quelque peu ennuyeux : contrôle des nouveau-nés, localisation d'animaux domestiques,

surveillance de bruits naturels, utilisations expérimentales et didactiques dans le domaine de la haute fréquence, etc..

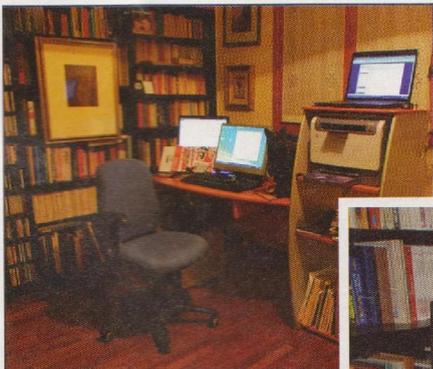
■ FAUTE AVOUÉE, À MOITIÉ PARDONNÉE

Ceux qui souhaitent disposer d'un téléphone espion complet, peuvent acheter chez NeoCall le Nokia N95 avec Neo-Suite 2K8 OS9 et Neo-Gps. C'est assez cher, 1 399 euros, mais ceux qui ne souhaitent que la Neo-Suite





pourront s'en tirer avec 499 euros. Vous pouvez aussi juste acheter certains modules : celui pour intercepter les Sms coûte entre 120 et 195 euros, selon le système d'exploitation Symbian. En ce qui nous concerne, nous avons justement testé le Nokia N95 avec la Neo-Suite 2K8 OS9 et Neo-Gps. Nous l'avons donné à un "cobaye", qui y a inséré sa carte Sim et l'a emmené avec lui au bureau. Nous l'avons tout de même averti qu'il s'agissait d'un téléphone espion et qu'il ne fallait pas trop dire de mal de nous lors de cette petite expérience.



Depuis notre rédaction, en milieu de matinée, nous avons donc commencé à agir. Pour nous dégourdir les doigts et les oreilles, nous avons appelé le téléphone espion avec notre téléphone "pilote", un mobile normal qui a toutefois été paramétré dans sa configuration initiale de sorte que le Nokia du cobaye le reconnaisse et accepte des commandes très spécifiques. Le téléphone espion a reconnu notre appel et a activé automatiquement

la communication : sans vibrer, sans qu'une lumière ne s'allume, sans sonner. Bref, sans donner de signe de vie. Mais en nous permettant d'écouter toutes les conversations dans le rayon d'action du micro du mobile. Au premier essai, pour dire la vérité, l'expérience n'a pas été très concluante vu que le cobaye était une femme qui, en tant que tel, le gardait dans son sac à main. On entendait un peu mais sans vraiment distinguer les mots. Une demi-heure plus tard, le son était nettement plus clair. Quoi de plus normal, puisqu'elle l'avait posé sur son bureau !

■ ESPIONNAGE TOUTS AZIMUTS

Après avoir brisé la glace en écoutant quelques commérages de bureau, nous avons envoyé au téléphone espion, via Sms, la commande qui permet d'intercepter les Sms de notre cobaye. Chaque fois qu'elle en recevait ou en envoyait un, ils arrivaient également sur notre mobile. Pas mal ! Et même, pas mal du tout, vu que selon une récente étude anglaise, la plu-

part des maris volages envoyant des textos tendres voir plus explicites sont découverts par leur partenaire grâce justement à ce système, en brisant ainsi les ménages. Nous envoyons un autre code via Sms (bien sûr le téléphone témoin ne les montre pas et ne les affiche pas parmi les autres Sms) pour recevoir une notification via Sms de tous les numéros des appels que notre amie a passés et reçus. Si votre fiancée appelle 18 fois le même numéro en l'espace d'une journée, et que ce numéro n'est ni le vôtre ni celui de sa mère, alors votre investissement dans un téléphone espion était-il sans doute justifié. En théorie, nous aurions pu également écouter ses appels, mais sa carte Sim aurait dû être activée pour la conférence (appels à trois). Malheureusement, elle ne l'était pas. Enfin, une procédure un peu plus difficile nous a permis d'activer la fonction du software Neo-Gps (199 euros, si vous l'achetez à part) qui permet de savoir dans quelle cellule se trouve le mobile espion, et donc de localiser sa position avec une certaine précision. Rien à dire si ce n'est qu'il s'agit d'un software très intéressant. Dommage qu'il ne soit absolument pas légal de l'utiliser pour espionner les gens.



ADVANCED PORT SCANNER 1.3

Le Port Scanning est une technique qui permet d'analyser les ports des ordinateurs d'un réseau local et d'établir lesquels sont ouverts, fermés, bloqués ou filtrés. Un port ouvert (ou "en écoute") indique qu'on peut se connecter à cet ordinateur. Lorsqu'un port est fermé ou bloqué, toute tentative de connexion est refusée.

PORT SCANNER

On parle en revanche de ports filtrés lorsqu'un pare-feu bloque son accès. Cette technique est habituellement utilisée par les administra-

teurs pour effectuer des contrôles et des opérations de maintenance sur le réseau local. Mais comment exécuter un Port Scanning ? C'est très simple

: il suffit d'un programme comme Advanced Port Scanner 1.3 pour détecter l'état des ports des PC de votre réseau. Voici comment faire.



 **icq**

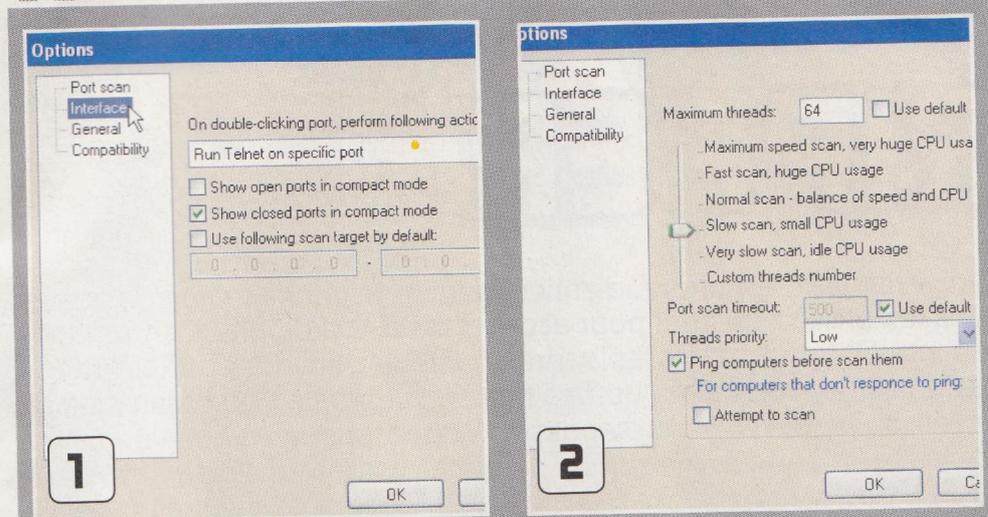


 **internet explorer**



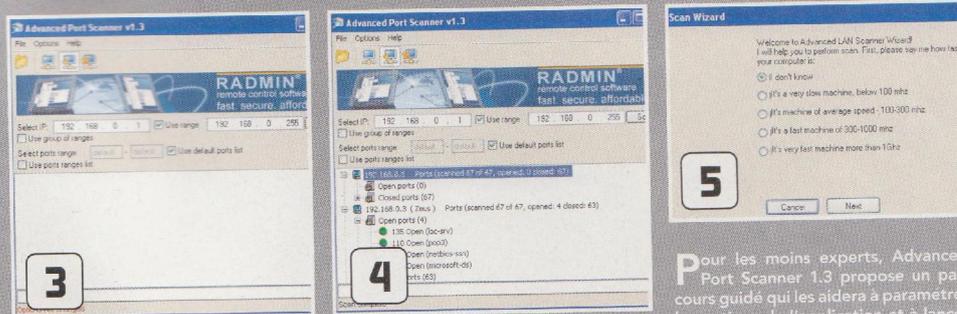
mail

TUTORIAL



1 Après avoir installé et lancé le programme, vous allez voir apparaître une petite interface. Advanced Port Scanner 1.3 dispose d'une fenêtre d'options de configuration qui s'ouvre en sélectionnant Configuration à partir du menu Options. Elle se subdivise en quatre sections activables en cliquant sur l'une des rubriques listées dans la colonne de gauche.

2 Cliquez par exemple sur Port scan. Là, vous pouvez paramétrer la vitesse d'analyse en déplaçant tout simplement la flèche disponible vers le haut ou vers le bas. Plus l'analyse du réseau sera rapide, et plus le processeur de votre ordinateur sera mis à contribution. Si vous souhaitez continuer à travailler pendant que le programme analyse le réseau, paramétrez une vitesse d'analyse moyenne-basse.



3 Pour lancer une analyse en un clin d'œil, tout ce que vous avez à faire, c'est entrer l'adresse IP de l'ordinateur que vous souhaitez analyser dans le champ Select IP. Sinon, tapez la première et la dernière adresse IP de votre réseau et cochez l'option Use range pour analyser tous les PC. À présent, cliquez sur Scan pour lancer le processus.

4 En fin d'analyse, vous pourrez voir le résultat dans la partie basse de l'interface. Chaque ordinateur voit spécifié le nombre de ports disponibles outre le nombre et le type de ports ouverts ou fermés. Pour afficher le détail des ports, cliquez sur le signe + qui se trouve à côté du message Open ports et Closed ports.

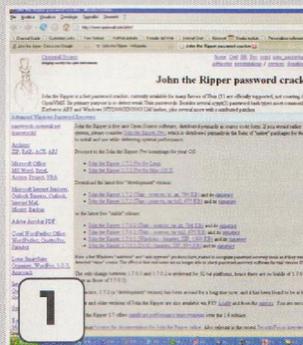
5 Pour les moins experts, Advanced Port Scanner 1.3 propose un parcours guidé qui les aidera à paramétrer les options de l'application et à lancer l'analyse. Pour cela, il convient de sélectionner Scan Wizard à partir du menu File. Concrètement, tout ce que vous avez à faire, c'est de répondre à quatre questions en sélectionnant la réponse parmi celles disponibles. À la fin, cliquez sur Scan pour lancer l'analyse avec les options réglées automatiquement par le programme.

JOHN THE RIPPER

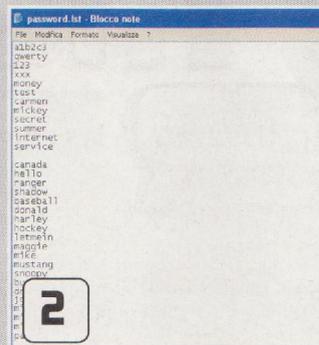
L'univers du PC est presque entièrement géré par des mots de passe. Vous les utilisez en effet pour accéder à votre ordinateur, entrer dans des sites Internet, dans les serveurs FTP ou encore pour accéder à des dossiers spécifiques ou des fichiers protégés. Pour vous assurer de la fiabilité de vos mots de passe ou en récupérer un que vous avez perdu, vous pouvez utiliser un programme de «crackage». Voici l'un des plus célèbres et efficaces : Jack the Ripper ! Il vous permettra de travailler sur les mots de passe Unix.

PASSWORD CRACKING

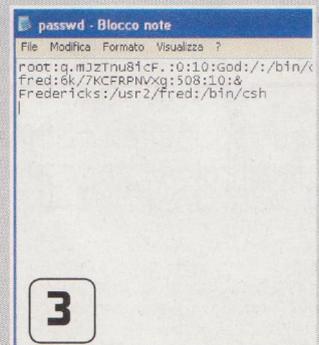
TUTORIAL



1



2

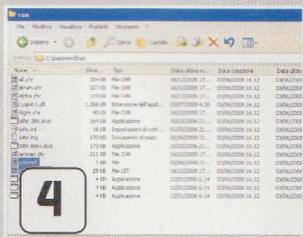


3

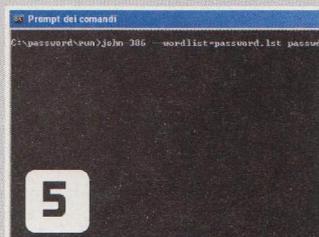
Développé au départ pour des systèmes d'exploitation Unix, ce programme est désormais compatible avec de nombreuses plates-formes dont celle de Windows que nous avons testée. Si la version du CD ne convient pas à votre configuration, consultez la page officielle de ce programme libre sur <http://www.openwall.com/john/>. Elle vous sera dans tous les cas utile pour trouver des infos et conseils. Pour tester et découvrir les mots de passe, John the Ripper combine différentes procédures de crackage et propose 4 modes de fonctionnement : Word List Mode, Single Crack Mode, Incremental Mode, et External Mode.

Le mode Word List est le plus accessible. Son fonctionnement est très simple : l'application tente d'associer au nom d'utilisateur en votre possession tous les mots de passe qu'elle trouve dans un fichier de référence (document que vous devez vous procurer et qui doit contenir le plus de mots-clés possible) jusqu'à ce qu'elle trouve le bon. Vous pouvez télécharger sur Internet le fichier password.lst, par exemple à partir du site www.openwall.com/passwords/wordlists/.

Placez le fichier password.lst dans le dossier contenant votre programme et insérez-y également le fichier passwd, un document Unix qui renferme toutes les informations sur les données d'accès. Ce document peut s'ouvrir avec le Bloc-Notes pour s'assurer qu'il contient bien des mots de passe Unix. Il doit être divisé en sept parties, dont chacune est séparée par deux points (:). Vous avez quant à vous besoin des deux premières parties (qui concernent respectivement le nom d'utilisateur et le mot de passe crypté). C'est ce fichier que John utilisera pour s'assurer que le nom d'utilisateur est associé au bon mot de passe.



4



5



6

Assurez-vous donc que le dossier du programme comprend les fichiers passwd et password.lst, puis ouvrez l'invite de commandes et entrez dans le dossier.

Lancez la recherche en tapant la ligne de commandes `john-386 --wordlist=password.lst passwd` et patientez. Le programme testera tous les mots qui se trouvent dans le fichier password.lst à la recherche du bon mot de passe. Le résultat sera enregistré dans le fichier john.pot qui restera vide si aucun mot de passe n'a été trouvé.

Dans certains cas, la procédure peut prendre pas mal de temps (surtout si vous avez de nombreux mots de passe à tester). Dans ce cas, vous n'êtes pas obligé de garder votre ordinateur allumé, vous pouvez interrompre la session de travail en appuyant sur CTRL+C et la reprendre dans un second temps avec la commande `john-386 --restore`.

PASSWORD CRACKING

CRYPTOCD

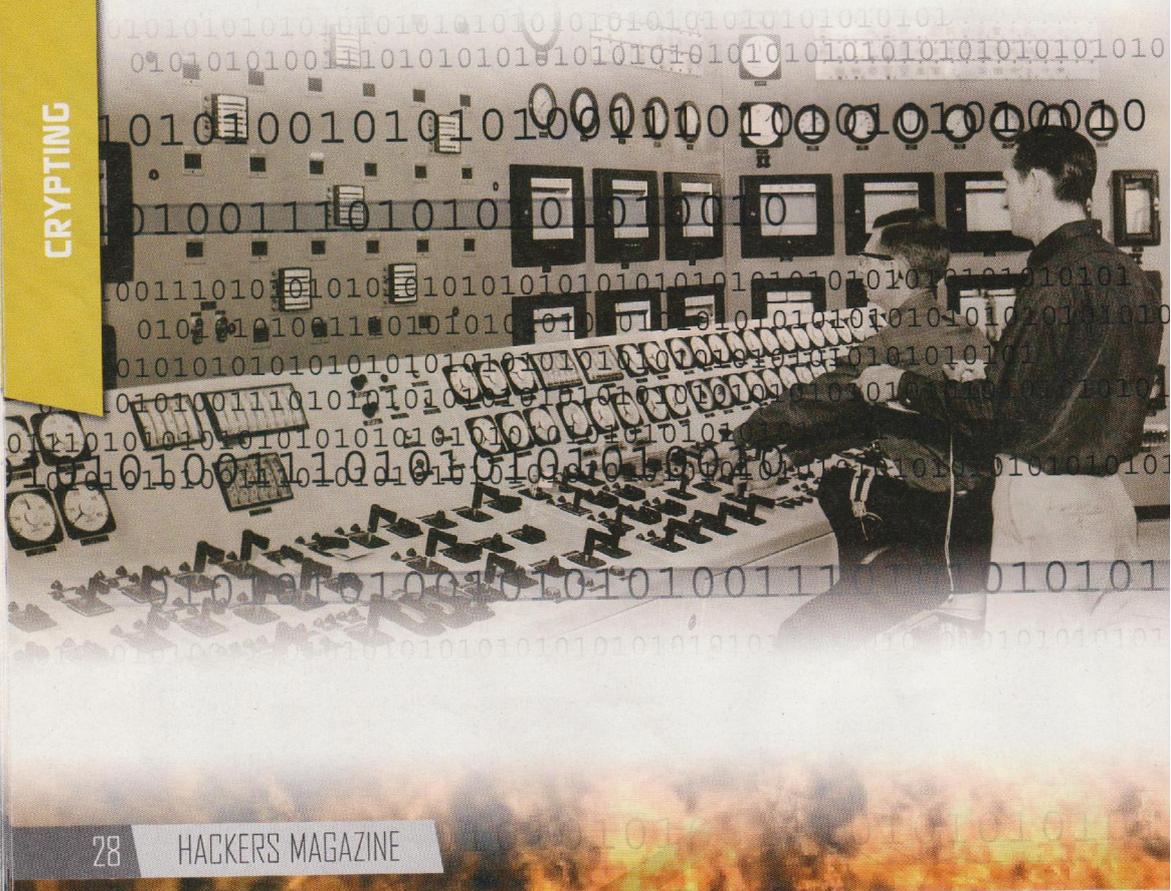
Vous souhaitez sécuriser au maximum les communications qui transitent via votre ordinateur ?

Ne cherchez pas plus loin, **CryptoCD est la solution qu'il vous faut !** Ce pack comprend en effet différents programmes dont l'objectif principal vise à renforcer le niveau de sécurité dans la

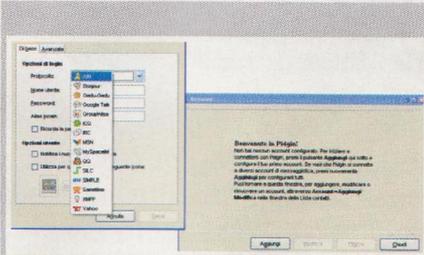
transmission de données via Internet. Il est en effet capable de gérer le cryptage des e-mails, de protéger les chats mais aussi votre anonymat lorsque vous surfez sur le Net. Pensé à l'origine pour le public allemand,

un peu d'intuition suffira néanmoins à l'utiliser, même si vous n'êtes pas familiarisé avec cette langue. Vous pourrez par la suite installer chaque programme en français ou en anglais.

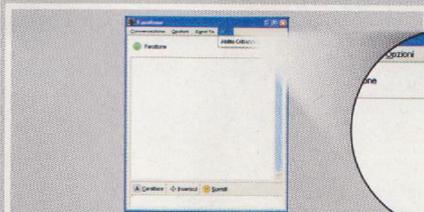
CRYPTING



TUTORIAL



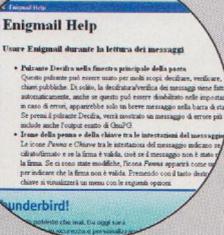
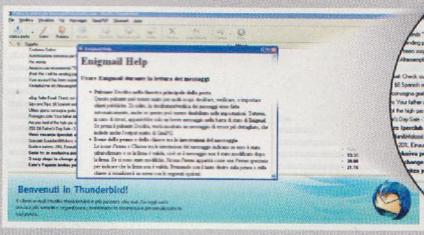
Concernant les messageries instantanées, CryptoCD inclut le programme Pidgin 2.3.1. et le module de sécurité pour crypter ses communications. Pidgin est un client de messagerie instantanée multi-protocole qui vous permet d'utiliser plusieurs comptes simultanément. Vous pourrez ainsi exploiter des applications comme ICQ, MSN Messenger, Yahoo, IRC, etc. dans un seul et unique programme avec une interface intuitive. L'utilisation de ce programme vous permet aussi d'économiser des ressources système par rapport à l'exécution simultanée de chaque client. Une fois Pidgin installé, vous devez choisir quels comptes inclure dans le programme. Nous vous conseillons d'insérer tous vos comptes habituels pour n'utiliser une seule interface.



Lancez ensuite l'exécutable de pidgin-encryption-3.0.exe et sélectionnez votre langue. Tout le reste est automatisé. Fermez puis relancez Pidgin et vous disposerez d'un outil de cryptage ou ne peut plus simple ! En cliquant sur le cadenas en haut, vous pourrez envoyer un message crypté ou non. Naturellement, pour échanger des messages codés, les autres utilisateurs avec lesquels vous dialoguez devront eux aussi avoir installé le plug-in.



Et pour protéger votre courrier électronique, voici Enigmail. Pour utiliser ce système, vous devez disposer du client Thunderbird et GnuPG (lui aussi inclus dans CryptoCD). Le CD offre une version d'Enigmail : si celle-ci n'est pas compatible avec votre système d'exploitation, vous pouvez en télécharger une autre sur <http://enigmail.mozdev.org/home/index.php>. Vous trouverez à cette même adresse une documentation fournie sur les paramètres du programme.



Après avoir installé Enigmail, vous trouverez dans la barre en haut de Thunderbird le nouveau menu OpenGP qui vous permettra d'accéder aux paramètres, à la gestion des clés et au guide du programme.



Concernant la protection sur Internet, CryptoCD laisse les commandes à Tor. Il s'agit d'un système de défense contre l'analyse du trafic : il empêche ainsi tout éventuel observateur de votre connexion Internet de découvrir les sites que vous consultez et interdit aux sites que vous consultez de savoir où vous vous trouvez réellement. Pour cela, il dévie vos communications à travers un réseau de relais, gérés par des volontaires éparpillés dans le monde entier. Pour plus d'informations sur le fonctionnement de Tor, allez sur <http://www.torproject.org/>.

CRYPTING

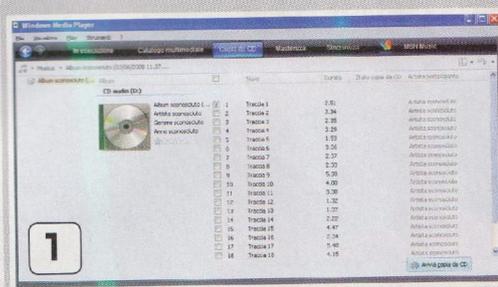
MP3STEGO

Si vous devez transmettre des infos personnelles via Internet à l'un de vos amis, écrire un e-mail ou encore envoyer un message à travers un programme de chat, méfiez-vous car ce n'est pas la meilleure solution ! Vous avez en effet de fortes chances d'être intercepté et de transmettre des informations confidentielles à des pirates ou, dans tous les cas, à des personnes qui vous sont totalement étrangères. Vous devez donc opter pour une méthode alternative afin de transmettre vos données en toute sécurité. Et MP3Stego est là pour ça !

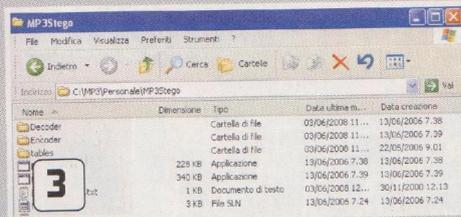
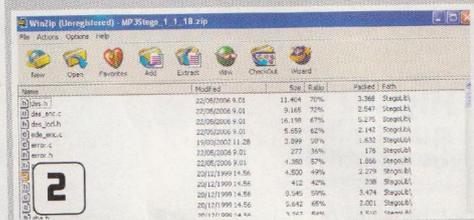
Ce programme vous propose en effet une méthode originale et fonctionnelle : cacher vos informations à l'intérieur d'un fichier Mp3 et les protéger avec un mot de passe. Voyons comment ça marche !

STEGANO

TUTORIAL

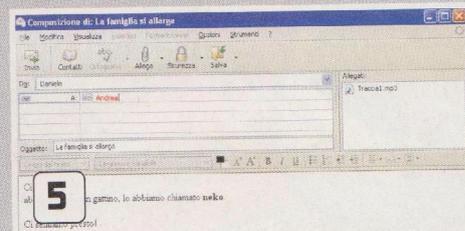


Tout d'abord, procurez-vous un fichier audio mono quelconque. Pour ce faire, prenez un CD audio et mettez-le dans le lecteur de votre ordinateur. Lancez Windows Media Player (déjà installé sur tous les PC tournant sous Windows) et cliquez sur le bouton Extraire la musique à partir du CD. Dans le menu Extraire, sélectionnez à présent la rubrique Options supplémentaires, puis cliquez sur l'onglet Extraire de la musique. Indiquez à présent le format d'exportation (WAV obligatoirement), et spécifiez dans quel dossier vous souhaitez enregistrer le fichier. Confirmez vos choix en cliquant sur OK et décochez toutes les cases sauf la première à côté du numéro progressif des pistes. Cliquez sur le bouton Démarrer l'extraction.



Vous trouverez MP3Stego dans le CD-ROM joint à la revue. Proposé au format compressé, vous n'aurez donc pas d'autre choix que de l'ouvrir avec un programme spécifique (avec Win-Zip par exemple) et d'extraire son contenu sur le disque dur.

Pour faciliter les choses, extrayez les dossiers du programme dans le dossier où se trouve le fichier WAV que vous avez extrait du CD, puis déplacez votre piste audio dans le dossier MP3Stego. Créez-y également un fichier texte (appelez-le par exemple infos_cachées.txt) où vous écrirez toutes les informations que vous souhaitez envoyer à votre ami.



Lancez à présent l'invite de commandes et allez dans le dossier MP3Stego. Tapez cette simple ligne de commande qui sert à convertir le fichier WAV en Mp3 et insérez le fichier texte en le protégeant avec un mot de passe (neko dans le cas présent) : encode -E infos_cachées.txt -P neko Pistel.wav Pistel.mp3. Après quelques secondes, vous trouverez le nouveau fichier Mp3 dans le dossier du programme, prêt à envoyer.

Avant d'envoyer le fichier à votre ami, assurez-vous que l'opération inverse fonctionne, à savoir celle qui consiste à extraire le fichier texte contenant les informations. Toujours dans la fenêtre de l'invite de commandes, tapez cette ligne de commande où vous spécifieriez le nom du fichier Mp3 qui dissimule les informations et le mot de passe que vous avez choisi : decode -X -P neko Pistel1.mp3. A la fin du processus, vous trouverez dans le dossier le fichier Pistel1.mp3.txt qui contient les informations que vous avez écrites. A présent vous pouvez donc envoyer immédiatement un e-mail à votre ami. N'oubliez pas de lui communiquer le mot de passe que vous avez choisi, en utilisant une phrase qui le contient mais sans le transmettre ouvertement, et de joindre le fichier Mp3 avec les infos.

Avant que le magazine ne soit interdit...
POUR TOUT SAVOIR SUR EMULE
mais pas seulement !

eMule & CO
LE MAGAZINE DES LOISIRS NUMÉRIQUES N°1

PRIX MALIN 2 €

TÉLÉCHARGER sur eMule,
LPHANT, EDONKEY, ETC.

- ✓ plus rapide
- ✓ plus facile
- ✓ plus discret

NOUVEAU N°1

→ PARAMÉTRER
LiveBox, NeufBox, FreeBox, HighID pour tous

→ COMPRENDRE
CHOISIR & INTÉGRER LA BONNE LISTE DE SERVEURS

→ ASTUCE
100 % ANONYME : MASQUER son identité

LE MATCH
Lphant :
Plus fort que la Mule ?
eMule & BitTorrent en un seul logiciel !

> À DÉCOUVRIR AUSSI...
Nos confidentiels • COPIER UN JEU VIDÉO
Les meilleurs MP3 & Vidéos • QUEL P2PISTE ÊTES-VOUS ? • Les mods d'eMule à la loupe
LES NOUVEAUX SERVICES MULTIMÉDIA ...

Soutenez nous, achetez le magazine !