PIRATE INFORMATIQUE N°7

LES CAHIERS DU HACKER

PIRATE INFORMATIQUE

NOUVELLE FORMULE ! AVEC CD GRATUIT > PLUS DE 50 FICHES PRATIQUES

Le PIRATAGE de A à Z

LE GUIDE PRATIQUE

HACKING / ANONYMAT
SURVEILLANCE /
MULTIMÉDIA /...

...S,
COPIE,
CRYPTAGE,
WEB
INTERDIT,
HACKING,
CRACKS,
DIRECT DL,
DÉBRIDAGE,
WI-FI,
MOT DE
PASSE,
JAILBREAK,
ANONYMAT,
BASE
DE DONNÉES,
PROXY,
MOBILE,
KEYLOGGER,
SPYWARE

COMMENT ÇA MARCHE [?]

HACKING

QUELS OUTILS POUR ESPIONNER SANS LAISSER DE TRACES ?

ANTI HADOPI

LES 8 SOLUTIONS QUI ÉCHAPPENT À LA SURVEILLANCE

INTERNET

DANGER : UN ACCÈS WI-FI CRACKÉ EN 5 MN PAR UN NEWBIE

SOMMAIRE

ANONYMAT

HACKING

PROTECTION

MULTIMÉDIA

MICRO FICHES

SPÉCIAL ESPION

LES CAHIERS DU HACKER
PIRATE INFORMATIQUE

N°7 – Nov 2010 / Janvier 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 :
Benoit Bailleul

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.

Édito

Vous aurez remarqué que ce nouveau numéro de *Pirate Informatique* a quelque peu changé. Notre nouvelle formule propose pas moins de vingt pages supplémentaires ainsi qu'un CD bourré de logiciels. L'autre nouveauté, c'est qu'à la demande générale, le magazine que vous tenez dans vos mains est davantage orienté «pratique». Plus de prises en mains, plus de trucs et astuces : *Pirate Informatique* devient le guide incontournable des nouveaux logiciels et tendances en terme de hacking et de sécurité informatique.

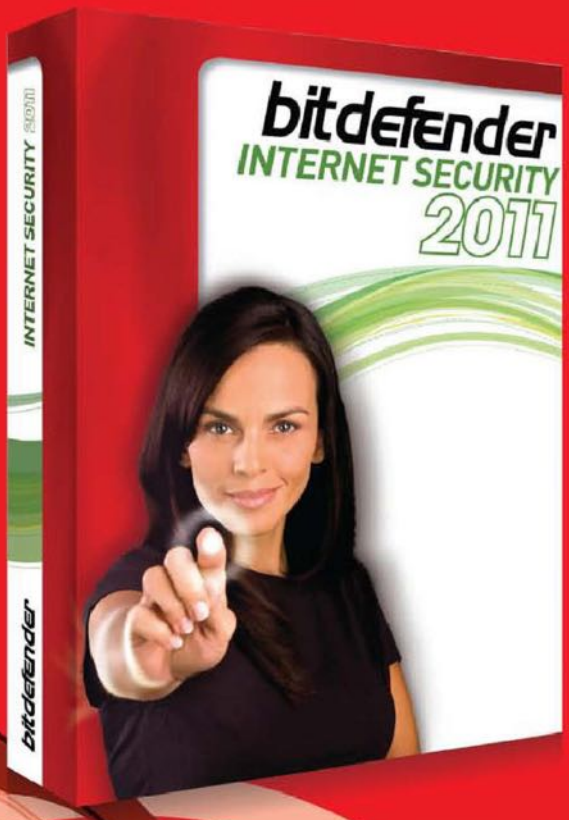
Nous remercions tous nos lecteurs qui ont permis à notre magazine de devenir le numéro un de sa catégorie en à peine un an. Désormais, tous les trois mois, vous retrouverez ce guide 100% pratique avec un panorama complet des dernières techniques et solutions. N'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions (redaction@idpresse.com).

Benoît Bailleul

bitdefender

GRAND CONCOURS

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

30 Licences à GAGNER !

Découpez ou recopiez sur papier libre ce coupon et envoyez-le à ID Presse :
27 Boulevard Charles Moretti - 13014 Marseille : ou par email sur concours@idpresse.com
Attention, OFFRE valable jusqu'au 31 décembre 2010 !

Nom : .....Prénom : .....

Adresse : .....

Question :

Les mises à jour automatiques des solutions BitDefender 2011 se font :

☐ Toutes les heures ? ☐ Toutes les semaines ? ☐ Tous les mois ?

Réponse sur : www.bitdefender.fr

0day : Désigne les cracks, keygen, appz ou exploit qui sont totalement nouveaux. Pour un pirate, une faille 0day signifie qu'elle n'a pas eu le temps d'être corrigée et qu'elle sera «sûre».

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

BBS : Les Bulletin Board System (littéralement «système de bulletins électroniques») sont (il en existe encore) des serveurs permettant des échanges de messages et de fichiers via un ou plusieurs modems reliés á des lignes téléphoniques. Populaire dans les années 1990, les BBS ont cédé la place á Internet.

Brute force : Méthode consistant á essayer tous les mots de passe jusqu'á 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 á la caisse. Il s'agit généralement d'un fichier EXE que l'on doit substituer á 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 où rend inopérant. Personnage très mal vu dans le milieu.

Darknet : Un darknet est un réseau privé virtuel qui a la particularité de stocker une partie des données sur les machines des participants. Les informations sont stockées, fragmentées et chiffrées pour que personnes ne puissent savoir qui héberge quoi.

DDoS : Le DoS (Denial of Service) est une attaque informatique qui consiste á envoyer des requêtes á un serveur afin de l'immobiliser, de le rendre inactif. Le DDoS (Distributed Denial of Service) est une variante qui utilise plusieurs ordinateurs coordonnés.

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 á un individu ou un logiciel malveillant d'exploiter une faille de sécurité dans un OS, un logiciel ou un jeu.

Full disclosure : se réfère á un principe de divulgation publique d'un problème de sécurité connu. Il s'agit en fait de faire connaître le problème pour que les utilisateurs ou exploitants soient avertis et puissent être sur leur garde ou remédier au problème.

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

Jailbreak : Opération qui consiste á trafiquer le système d'exploitation d'un appareil pour avoir accès á des paramétrages 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.

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

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

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.

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.

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

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.

White hat : Un white hat, á l'inverse des black hat, sont de «gentils» hackers qui prônent pour le full disclosure. Leur but n'est pas d'exploiter les failles mais de les chercher pour les rendre publiques et alerter l'opinion.

LEXIQUE

HADOPI :

les solutions qui échappent à la surveillance

Les premiers mails d'avertissement seront bientôt dans les tuyaux ! Des milliers d'internautes français vont enfin « bénéficier » des remontrances de Hadopi. Les échanges de fichiers sur les réseaux P2P seront sous surveillance... mais d'autres solutions de partage sont pour l'instant oubliées par le législateur. Du coup, les habitudes de téléchargement risquent d'être profondément modifiées.

TMG va bientôt commencer sa chasse aux socière ! Cette société (Trident Media Guard) a été retenue par les ayants-droit pour surveiller et collecter les adresses IP des internautes soupçonnés de téléchargements illégaux. Attention, seuls les échanges de type P2P seront dans un premier temps surveillés. Et les réseaux les plus populaires seront bien sûr les plus contrôlés. Ainsi, Kad/eDonkey (eMule), BitTorrent (µTorrent, Vuze, etc.), Gnutella (LimeWire), Ares, Piolet et Soulseek seront prioritairement dans le collimateur des Sacem, SPPS et autre Alpa. Ca tombe bien, il s'agit là des réseaux les moins sécurisés et les plus faciles à surveiller ! Donc aucune excuse pour ne pas se faire prendre...

Les règles du jeu

On apprend aussi que ce ne sont pas tant les téléchargements que la mise à disposition de fichiers illégaux qui sera surveillée. Quand vous téléchargez un fichier, les parties du fichier final que vous récupérez sont aussi accessibles aux autres internautes (c'est le principe du P2P, tout le monde est à la fois émetteur et récepteur). On notera que ceux qui configurent leur logiciel pour ne jamais partager les fichiers en cours de téléchargement ou déjà rapatriés sur leur disque dur semblent plus protégés que les autres. Hadopi favorise les pirates égoïstes ! Attention, d'autres solutions existent pour éviter les fameuses lettres et passer entre les mailles du filet...

Toujours en retard...

Relevé par la Quadrature du Net, un vice de forme s'est glissé dans la mécanique (bien huilée ?) d'HADOPI. En effet, l'ARCEP n'a pas été consulté comme le stipule le Code des Postes et Communications Électroniques. Le président d'un petit FAI associatif a alors déposé un recours suspensif devant le Conseil d'État histoire de ralentir encore un peu plus la machine....

Le stream aussi ?

Hadopi est un projet de loi qui vise à enrayer le téléchargement illégal mais ce projet de loi serait aussi applicable au monde du streaming ! C'est le secrétaire général de l'ARMT qui est à l'origine de cette déclaration. En effet, le texte est d'après lui destiné à l'ensemble des réseaux. Les «streamers» peuvent néanmoins dormir tranquille : quand on voit le temps qu'il faut à Hadopi pour faire partir les premières lettres...

L'autoroute de l'information

Pour sa première campagne de sensibilisation, l'Hadopi a choisi le retour des vacances. Les week-ends du 20 au 22 août et du 27 au 29 août, quelque 260.000 dépliants explicatifs ont été distribués aux péages des autoroutes. Ces dépliants visent à délivrer «le mode d'emploi» de l'Hadopi : le fonctionnement, la riposte graduée et les risques encourus.

SOLUTION 1

Le Stream > Ne téléchargez plus !

Le streaming, c'est un peu la méthadone du P2P. Idéal pour se sevrer et essayer de gérer le manque dans les meilleures conditions. Ce n'est pas aussi bandant (un écran de PC, c'est sympa mais bon) et ce n'est pas non plus la même qualité mais au moins ça n'inquiète pas vos proches. Et, surtout, de plus en plus d'offres légales fleurissent sur le marché. Pour la musique, il faut vraiment faire preuve de mauvaise volonté pour ne pas trouver son bonheur (**Deezer**, **Spotify**, etc.) Quand aux films et séries, il faut reconnaître que 80 % des dealers ne semblent pas en règle avec la loi. Mais cette loi, justement, ne peut pas punir le simple consommateur... puisqu'il n'y a pas de téléchargement. Des sites comme **DpStream**, **Stream-easy** ou **Lookiz** proposent des milliers de films, séries, documentaires et animes en accès libre et en toute impunité. Les ayants-droit, pour contrer ce phénomène, n'ont que deux options : attaquer les sites éditeurs et exiger leur fermeture ou négocier... Quand à l'internaute, il peut s'installer tranquillement devant son écran en attendant la fin du match.

PRATIQUE ▸ Les solutions pour contourner MegaVideo

Le site d'hébergement et de streaming MegaVideo limite le visionnage de ses vidéos à 72 minutes, pour inciter à souscrire à un compte Premium. Il existe cependant plusieurs techniques permettant de contourner cette limitation.

Changement d'IP
Feinte de sioux

Cette technique s'adresse surtout aux Internautes possédant une IP dynamique. Commencez par effacer les «cookies» de vos navigateurs (sous Firefox allez dans **Outils** et choisir **Effacer mes traces** puis cochez **Cookies**, cliquez enfin sur **Effacer mes traces maintenant**). Déconnectez-vous et reconnectez-vous ou débranchez et rebranchez votre box. Votre connexion réinitialisée vous offre une nouvelle IP. Retournez sur la page, actualisez et reprenez le téléchargement où vous l'aviez stoppé. Le tour est joué.

Le + Fonctionne bien avec les IP dynamiques

Le - Pénible de reprendre le streaming après une interruption

CacheViewer / Gagne à être connu

CacheViewer est une petite extension Firefox très pratique. Une fois que vous l'avez téléchargée (**http://bit.ly/4389cP**) et installée, elle vous permet de visualiser et récupérer ce qui se trouve dans la mémoire cache de votre navigateur. Pour cela, vous devez laisser la vidéo se charger complètement, elle se retrouve alors dans la mémoire cache, affichez-la avec CacheViewer et sauvegardez-la sur votre ordinateur.

Le + Il fallait y penser

Le - Perd tout le charme du streaming puisqu'il faut attendre le chargement complet de la vidéo.

Illimitux / «50/50»

Voici une autre extension de Firefox qui a fait parler d'elle. Ce petit add-on permet de faire sauter les limitations présentes sur plusieurs sites de streaming dont MegaVideo. Téléchargez l'utilitaire ici : **http://bit.ly/19tGR2** et installez-le. Il suffit ensuite de lancer la vidéo sur MegaVideo. Le plugin se charge de modifier votre IP pour que vous puissiez continuer à lire le film.

Le + Très simple d'utilisation

Le - MegaVideo a trouvé une parade et Illimitux ne fonctionne qu'une fois sur deux.

SOLUTION 2

Le P2P privé > Entre potes...

Le « F2F », comprenez Friend-to-Friend (partage entre amis), ne sera jamais une solution massive d'échanges de fichiers (quoique OneSwarm permet de se faire des amis de manière exponentielle). Par définition, ce type de service permet à un groupe restreint de se retrouver dans un espace privé pour partager leurs documents. Pour rentrer dans ce groupe, il faut être accepté et donc montrer patte blanche. Idéal pour les échanges de fichiers volumineux dans le cadre professionnel ou entre amis. Aucune solution de surveillance automatisée ne peut intercepter ces échanges puisqu'il faudrait se placer à l'intérieur de ce cercle privé. Le plus connu de ces logiciels est **GigaTribe**. Mais d'autres commencent eux aussi à faire parler d'eux et développent de nouvelles fonctionnalités pour enrichir l'esprit communautaire (intégration d'outils comme Skype, MSN, Facebook, etc.) On

citera notamment : **Weezo et Peer2Me**. Ces solutions ne permettent pas aux internautes d'accéder à des médiathèques gigantesques puisque le nombre de participants est limité au sein de chaque cercle d'amis. Mais c'est un outil idéal pour ceux qui veulent par exemple créer ou rejoindre une communauté de 20, 30 ou 50 internautes échangeant des fichiers sur une thématiques précise.

PRATIQUE ▸ OneSwarm, des amis anonymes ?

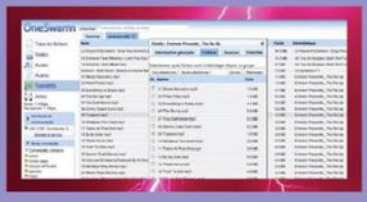
Permettant de protéger sa vie privée mais aussi d'éviter les fameuses lettres envoyées par HADOPI, OneSwarm est un logiciel F2F (friend-to-friend) qui fonctionne sans pour autant nécessiter d'amis de confiance dès le début...

1 Premiers pas

Au démarrage, le logiciel va ouvrir une nouvelle page dans votre navigateur. Cliquez ensuite sur **Utiliser les paramètres par défaut**. Dans la colonne de gauche, cliquez sur **Ajouter des amis** si vous avez un pote qui souhaite commencer l'aventure avec vous ou si vous vous faites parrainer. Il est possible d'ajouter des amis depuis Gmail, depuis votre réseau local ou manuellement avec des clés publiques (qu'un ami vous aura envoyé par e-mail). Vous pouvez aussi inviter un camarade à vous rejoindre dans cette même colonne gauche, en bas. Même si vous êtes seul, vous êtes connecté d'office au server de communauté UW CSE Community Server...

2 Télécharger

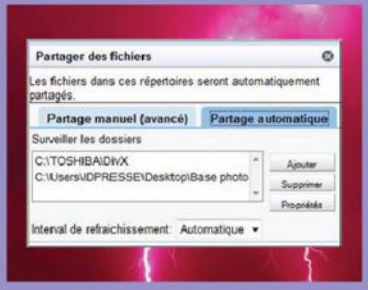
Le problème c'est qu'avec cette méthode, votre progression risque d'être lente puisque personne ne vous fait confiance. Il faudra,



en effet, avoir des fichiers très demandé pour grappiller quelques clés publiques. Si vous êtes nouveau sur le réseau, il est donc plus facile de commencer avec un parrain ou un ami qui ne sera pas en **Limited friend**. Cette personne sera chargée de vous tester pour évaluer votre fiabilité (voir encadré) et la qualité de vos fichiers. Vous faites bien sûr de même pour elle ! Pour rechercher un fichier, il suffit de taper ce que vous voulez dans le champ en haut puis de taper sur **Entrée**. Dans la liste, cliquez sur ce qui vous intéresse puis sur **Télécharger**. Ces fichiers iront dans votre dossier **Documents>Oneswarm Downloads**. N'oubliez pas de partager aussi ce dossier !

3 Partager

Pour le partage, il est conseillé de créer un dossier de partage automatique. Dans l'interface, cliquez sur **Partager** puis dans la fenêtre qui s'ouvre il faudra aller dans **Partage automatique**. Recherchez le dossier que vous voulez partager puis validez. Choisissez



Grouped Media Files only puis faites **Save**. Répétez l'opération avec autant de dossiers que vous voulez.

SOLUTION 3

Le téléchargement direct
> Acheter sa tranquillité!

MegaUpload, c'est le 45e site le plus visité en France (source : Alexa.com). Depuis deux ans, son ascension est irrésistible et il pourrait devenir rapidement le premier service d'échanges de fichiers en Europe. Ici, on ne parle pas de P2P mais de téléchargement direct : les internautes téléchargent des fichiers qui sont directement sauvegardés sur les serveurs de la société MegaUpload. Du coup, les vitesses de transfert sont 10 fois plus rapides qu'avec le Peer-to-peer. Surtout, comme il n'y a pas d'échanges de pair à pair (entre internautes), la surveillance actuelle de TMG est inopérante. MegaUpload, comme son principal concurrent

RapidShare, pousse même le vice jusqu'à proposer un mode de connexion sécurisé de type SLL : l'adresse IP et le type de données transférées sont invisibles pour la personne qui parviendrait à intercepter le flux.
Sur MegaUpload et RapidShare, ce sont les internautes qui uploadent les fichiers sur les serveurs de ces sociétés. Des liens de téléchargement sont automatiquement générés et se retrouvent rapidement sur des sites, blogs et annuaires spécialisés (comme **Moviz** ou **Liberty Land**). Mais cette « qualité » de service a un coût : en mode gratuit le nombre de téléchargements est limité à un par jour (avec une taille max de 2 Go pour MegaUpload). Il faudra opter pour

un compte Premium (20 € pour 3 mois par exemple sur MegaUpload) pour bénéficier d'un accès illimité. Et ils sont de plus en plus nombreux à estimer que cela vaut le coup. Pourtant, ce type de service est dans le collimateur de la justice et les internautes pourraient bientôt être inquiétés. Certains ayants-droit ou producteurs (comme l'intellectuel Marc Dorcel) ont déjà expliqué qu'une traque sur les réseaux MegaUpload pouvait et avait déjà été effectuée en interne, à des fins de « pure observation ». Autres sites de téléchargements directs qui défraient la chronique : **HotFile**, **Zshare**, **MediaFire**, **Deposit**, ...

SOLUTION 4

USENET > Le méconnu incontrôlable

On parle là aussi de téléchargement direct mais le protocole Usenet est différent de ceux utilisés par MegaUpload ou RapidShare. Ici, on télécharge des « binaries », des fichiers morcelés en dizaines de petites parties qu'il faut ensuite agréger. Ces « binaries » sont héritées d'un protocole qui date de plus de 30 ans et qui était utilisé à l'origine pour l'échange d'informations textuelles. Moins intuitive, son utilisation paraît beaucoup plus complexe que ses rivaux pour un béotien mais Usenet possède sa communauté d'inconditionnels. Les deux services leaders pour accéder à Usenet son **GigaNews** et **Usenext**. Sachez que **Free** possède son propre service d'accès gratuit aux Newsgroups pour ses abonnés. Mais le choix est ici plus limité.

SOLUTION 5

LES VPN > Les tunnels de la contrebande

Les internautes qui ne veulent pas abandonner leur logiciel P2P préféré ont forcément entendu parler des VPN (Virtual Private Network > Réseau privé virtuel). **Ipredator** et **Ipodah** ont fait les choux gras de la presse l'année dernière et ont été créés spécifiquement pour déjouer les outils de surveillance. Présentés comme des solutions dédiées à BitTorrent, ils sont en fait compatibles avec tout logiciel qui envoie et reçoit des données sur le Web. Un VPN va prendre en charge ses données et les « encapsuler », les faisant transiter dans une sorte de tunnel virtuel jusqu'à votre destinataire, passant par de nombreux relais. Personne ne saura d'où viennent ces données et ce qu'elles contiennent. Par contre, qui dit multi-relai dit aussi vitesses de transfert plus limitées.
Pour le P2P, nous avons repéré les meilleures offres actuelles dans le tableau ci-contre. La plupart d'entre eux sont payants mais vous pouvez toujours tenter votre chance ou essayer avec un VPN gratuit.

SOLUTION 6

Les Darknet
> Le Saint Graal de l'anonymat

Utiliser un réseau crypté pour échapper à Hadopi, c'est un peu se servir d'une sulfateuse pour tuer une mouche : disproportionné et peu pratique. Pour ceux qui parviennent à les maîtriser, c'est le nec-plus-ultra pour protéger sa vie privée et son Internet. Mais ces grosses berta n'étant pas spécifiquement dédiées aux échanges de fichiers, cela implique qu'il vous faudra un peu de temps pour apprivoiser ces technologies. Seuls les plus paranos devraient s'y risquer. Parmi les solutions les plus connues, on citera **Tor**, **Netsukuku**, **Freenet** et **Darknet.me**.

SOLUTION 7

Seedbox et compagnie...
> C'est pas moi, c'est l'autre

Une seedbox est un serveur dédié équipé d'une ligne à haut débit en fibre optique utilisé exclusivement pour les téléchargements BitTorrent. Ce serveur s'occupe de récupérer le fichier sur le Web comme un logiciel classique (µTorrent, Vuze, etc.). Une fois que la seedbox aura achevé le travail de téléchargement, vous pourrez vous connecter à ce serveur pour rapatrier votre fichier sur votre disque dur. La première étape se fait donc en ultra-haut débit (rapatriement du fichier sur un serveur distant, la fameuse Seedbox), la deuxième étape se fait en téléchargement direct : depuis la seedbox vers votre PC (sans limitation de vitesse donc). Certes, vous téléchargez en fait le fichier deux fois mais beaucoup plus rapidement qu'avec un download classique de type P2P ! Surtout, c'est l'adresse IP de la seedbox qui se connecte à BitTorrent, l'internaute est donc protégé de toute surveillance. Beaucoup de services seedbox sont payants (comme **Torrenflux** et **Seedbox Hosting**) mais certaines solutions gratuites apparaissent, comme **Torrific** et **Leechpack**.

SOLUTION 8

LE P2P CRYPTÉ > Le P2P 2.0

Ces solutions sont assez récentes et répondent aux besoins du grand public : conserver ses habitudes de téléchargement avec des logiciels qu'il connait tout en bénéficiant de la protection offerte par les réseaux cryptés destinés généralement aux plus aguerris des internautes. Plus simples et plus automatisés, ces solutions de P2P cryptés concernent notamment eMule, LimeWire et BitTorrent. On évoquera notamment **I2P** qui est une solution de cryptage intégrant trois logiciels dédiés : **iMule** pour eMule, **I2Phex** pour le réseau Gnutella et **I2PSnark** pour BitTorrent. Ce dernier bénéficie aussi d'un excellent logiciel qui devrait séduire nombre d'internautes : **BitBlinder,** terriblement simple à utiliser, très efficace et offrant un niveau de sécurisation rarement atteint pour une solution grand public. Enfin, très proche de l'interface d'eMule, il faut citer un logiciel qui bénéficie d'une certaine notoriété : **StealthNet**, basé sur le réseau protégé **rShare**.

PRATIQUE ▸ Restez anonyme avec StealthNet

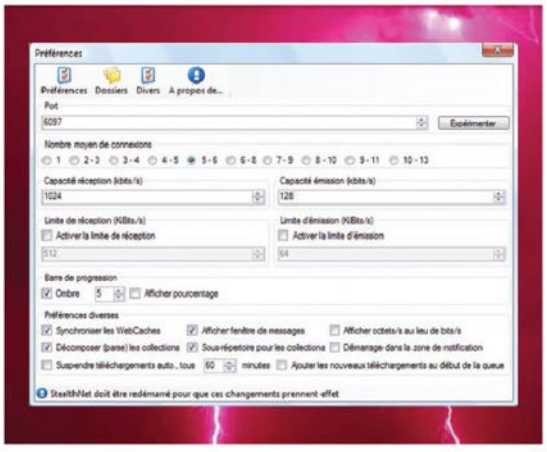
L'espionnage des réseaux augmente de jour en jour, et vos échanges P2P pourraient très bien être surveillés en ce moment même. Heureusement, en parallèle, le P2P anonyme se développe. Sur StealthNet, votre identité et vos échanges sont masqués...

1 La barrière de la langue

Cliquez en haut à droite sur l'onglet **Einstellungen**. Cliquez ensuite sur **Verschiedenes**, sélectionnez **Französisch**, puis fermez la fenêtre. Redémarrez le logiciel et l'interface est maintenant dans la langue de Molière !

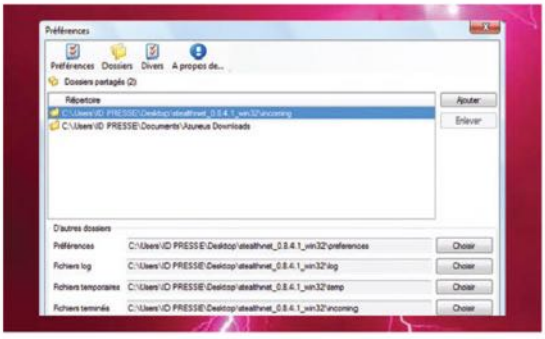
2 Le réglage des paramètres

Rendez-vous dans l'onglet **Paramètres,** puis **Préférences.** Le port 6097 est indiqué par défaut. Pour optimiser le fonctionnement de StealNet, vous devez ouvrir ce port sur votre box ou votre routeur. Si vous possédez un autre logiciel P2P, le plus simple est de remplacer le chiffre 6097 par celui correspondant au port TCP que vous avez déjà ouvert dans ce logiciel. Par exemple, pour eMule, vous trouverez ce numéro dans **Préférences** puis **Connexion**. Dans ce cas de figure, vous ne devrez pas utiliser StealNet et eMule en même temps.



3 Partager ses téléchargements

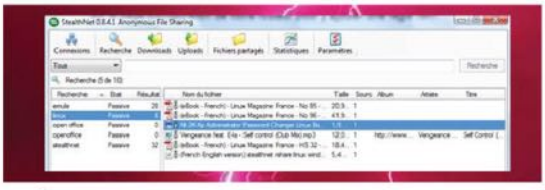
Toujours dans **Paramètres,** cliquez sur l'onglet **Dossiers,** puis sur le bouton **Ajouter**. Parcourez votre disque dur et choisissez les



dossiers que vous souhaitez mettre en partage. N'hésitez pas à partager un maximum de fichiers..

4 Télécharger un fichier

Rendez-vous dans l'onglet **Recherche**. Tapez votre mot-clé dans la zone dédiée. Soyez patient, les résultats mettent entre 2 et 5 minutes à apparaître.
Double-cliquez sur le fichier qui vous intéresse et retrouvez l'avancement dans l'onglet **Download** !



QUI VEUT SE CACHER sur Internet ?

De plus en plus de personnes désirent ne plus être traçables sur le Net. Qu'il s'agisse de dissident politique ou de citoyen lambda désireux de préserver leur vie privée, l'anonymat devient un véritable besoin. Quels sont les outils mis à disposition des internautes, comment se protéger et quels sont les risques ?

La Chine, l'Iran, la Biélorussie mais aussi une quantité d'autres pays pointés du doigt par Reporters Sans Frontières (RSF) ne respectent pas la liberté de la presse, musellent les opposants, surveillent ou censurent le réseau des réseaux. La situation est telle que RSF a inauguré en Juin dernier un «Abri anti-censure». Il s'agit d'un un lieu destiné aux journalistes ou blogueurs dissidents permettant d'apprendre comment contourner la censure et conserver leur anonymat sur Internet. Bien sûr pour les personnes qui ne peuvent pas faire un saut à Paris pendant le week-end RSF s'est associé avec l'entreprise de sécurité des communications XeroBank pour mettre gratuitement à disposition des utilisateurs un VPN sécurisé (Virtual Private Network). Il suffira de demander l'accès à RSF pour obtenir un code d'accès et une clé USB «magique» qui permettront d'avoir accès au VPN sans pour autant avoir de connaissance technique.

Le Parti Pirate s'y met aussi !

Ce n'est pas la seule initiative du moment puisque le fameux Parti Pirate suédois y est aussi allé de sa petite contribution. Très impliqué dans la défense des libertés individuelles, ce dernier a récemment publié un petit guide à l'attention de l'opposition iranienne où il explique comment crypter ses communications pour ne pas se retrouver dans une des somptueuses geôles de Téhéran. Pour ce faire le Piratpartiet (en suédois dans le texte) a configuré 3 nœuds permettant d'utiliser le logiciel TOR et un serveur proxy. Si les utilisateurs veulent poser des questions au Parti mais qu'ils ont peur d'être espionnés, il est aussi possible de les joindre via un email chiffré grâce à la clé PGP publique disponible sur cette page : **www2.piratpartiet.se/proxy_eng**. Comme d'habitude, ils ont pensé à tout !

Le filtrage pointé du doigt

Guillaume Champeau, webmaster du site Numerama.com a coécrit le livre *Confession d'un pédophile, l'impossible filtrage du Net* avec un collectif d'auteur. Cet ouvrage entend démontrer que la LOPPSI (Loi d'Orientation et de Programmation pour la Sécurité Intérieure), au lieu de lutter contre la pédophilie sur Internet grâce à des méthodes de filtrage, pourrait faciliter les dérives mafieuses liées à ce business...

www.ilv-bibliotheca.net

L'IP de la discorde

Lorsque l'on navigue sur Internet, l'ordinateur utilise une adresse unique, appelée adresse IP, permettant aux serveurs Web distants de recevoir des données et de lui répondre. C'est donc le moyen qu'ont les gouvernements pour retrouver la trace des dissidents (terroristes !) ou des méchants téléchargeurs (terroristes !). Même si la plupart du temps l'adresse IP fournie par le FAI et change à chaque nouvelle connexion, ce dernier garde un fichier journal qui permet de faire une correspondance entre vous et ce que vous faites sur le réseau !

LES OUTILS pour devenir invisible !

Sans forcement être recherché par la police politique chinoise ou par les ninjas de la mort d'HADOPI, vous désirez simplement protéger votre vie privée et ne pas laisser de trace sur Internet ? Suivez le guide...

MÉTAMOTEUR

IXQUICK > Recherches anonymes

Tous les moteurs de recherche scrutent et enregistrent vos recherches sur la Toile. Même si vous n'avez pas forcement quelque chose à cacher, retrouver vos traces de surf sur Internet n'est pas vraiment confidentiel. Avec Ixquick, surfez en tout anonymat ! Ce métamoteur va puiser ses résultats chez Google, Ask ou Bing pour vous donner le meilleur. Ixquick permet par ailleurs de forcer l'établissement d'une connexion sécurisée HTTPS à ses serveurs pour éviter le regard des curieux...

http://ixquick.com

PROXY

YOUHIDE > Surf anonyme

YouHide est un proxy qui permet de se connecter à n'importe quel site de manière anonyme. Votre IP n'est jamais logguée, c'est l'IP de YouHide qui le sera. Comme il s'agit d'un proxy PHP, les sites qui demandent un enregistrement fonctionneront sans problème. Plus rien ne vous trahira lorsque vous surferez sur le site de «Plus belle la vie»...

www.youhide.com

PROXY

NETSCOP > Surf Anonyme

Dans la même veine que YouHide, voici Netscope. La seule façon d'effectuer un surf anonyme consiste à passer par un serveur intermédiaire qui se connectera aux sites web que vous visitez à votre place et vous renverra à son tour les pages. Ce serveur est dit mandataire ou «proxy». Pour votre fournisseur d'accès vous vous connectez toujours au même serveur et pour le site distant, vous n'existez pas ! Il faudra juste s'attendre à un temps de connexion plus long car les paquets de données doivent circuler de votre ordinateur au proxy, du proxy au site web, puis la même chose en retour...

www.netscop.net

SUPER PROXY

TORPARCK > Navigateur

Les internautes soucieux de la protection de leur vie privée apprécieront sans doute le navigateur Torpark. Celui-ci, basé sur la version 1.5.0.7 de Firefox Portable permet de surfer sur Internet sans laisser la moindre trace identifiable de son passage, que ce soit sur les sites visités ou la machine utilisée pour se connecter à Internet. Torpark chiffre toutes les données émises et reçues par l'utilisateur et se connecte aux sites Web visités par l'intermédiaire du réseau TOR, ce qui permet de dissimuler la véritable adresse IP de la machine utilisée. À l'instar du logiciel

Portable Firefox dont il est dérivé, Torpark peut être exécuté depuis une clé USB et aucune installation n'est requise. Une fois la clé USB débranchée, il ne subsiste donc aucune trace de la navigation sur Internet, ni cookie, ni historique, ni fichiers temporaires. Ce navigateur furtif a été mis au point par un groupe de « hacktivistes » qui militent pour le droit au respect de la vie privée des internautes.

www.youhide.com

SERVICE WEB

IPFUCK > Fausses IP

Vous avez sans doute déjà entendu parlé du logiciel Seedfuck. Voici l'extension IPFuck pour Firefox qui débarque ! Ce plugin permet de générer de fausses adresses IP censées détourner l'attention des futurs trackers de l'Hadopi. En clair, un site ou un serveur visité va enregistrer 4 connexions

différentes dont trois seront complètement fausses. Il s'agit donc d'essayer de pourrir le réseau avec des IP contrefaites et mettre la société Trident Media Guard dans l'embarras...

http://ipfuck.p4ul.info

Tor, le Super Proxy

Tor est un logiciel qui dissimule votre IP derrière une chaîne de serveurs dite de «routage en oignon» (organisée en couches). Ce système a été conçu pour combler les carences des serveurs mandataire (proxy). Ici, les communications rebondissent au travers d'un réseau de serveurs appelés "onion routers"....

Avec Tor, tout est décentralisé et chaque intervenant ne peut pas savoir ce qui passe par sa machine ! Il est donc impossible d'imaginer des attaques «man in the middle» (dans le cas où un curieux se glisserait dans le système pour l'étudier de l'intérieur). Vous êtes ainsi protégé contre les sites Web qui enregistrent les pages que vous visitez, contre les observateurs externes, et même contre les "onions routers" eux-mêmes puisque seul le premier nœud du circuit connaîtra votre adresse IP. Tor fonctionne avec tous les navigateurs mais le plugin Torbutton sous Firefox est très pratique. Attention, il y a un inconvénient : Tor fait diminue drastiquement la vitesse de connexion… À essayer tout de même.

CE QU'IL VOUS FAUT

> Tor software (gratuit)

www.torproject.org

DIFFICULTÉ

PRATIQUE ▶ Une navigation anonyme avec TOR

1 L'installation

Après avoir téléchargé, lancez l'installation. Si vous utilisez Firefox, sélectionnez **Torbutton** et choisissez le dossier par défaut. Une fois que le processus d'installation est terminé, appuyez sur **Suivant** et enfin sur **Terminer** en laissant la case **Démarrer les composants installés maintenant**. Si votre connexion est protégée par un pare-feu, il vous faudra la configurer afin d'autoriser Tor et Privoxy

à se connecter à Internet. Normalement un message de votre firewall devrait s'afficher et vous devrez confirmer l'exception.

2 La fenêtre principale

Dans le systray (les icônes à côté de la pendule Windows), deux icônes sont normalement apparues : une en forme d'oignon (Tor) et une ronde avec un P sur fond bleu (Privoxy). Double-cliquez sur l'icône Tor, une

fenêtre s'ouvre contenant trois parties. En haut vous pouvez voir si Tor est actif et au milieu vous pourrez gérer les relais (ou «onion router»).

3 Certaines options

Voir le réseau vous permet de voir par quels serveurs vous passez. Vous pouvez aller y faire un tour si vous êtes curieux. **Utiliser une nouvelle identité** sert tout simplement à faire croire que vous venez de vous connecter. Pratique si votre connexion est devenue trop lente. **Graphe bande passante** permet de suivre l'évolution de votre bande passante et Journal des messages enregistre tout ce qui se passe avec Tor, y compris les erreurs. N'allez dans les **Paramètres** que si vous êtes sûr de votre coup. Normalement, il n'y a rien à modifier ici.

4 Avec Internet Explorer

Si vous n'utilisez pas Firefox, vous n'aurez pas à disposition le Torbutton (dans le coin inférieur droit de votre fenêtre Firefox) qui permet d'activer ou de désactiver Tor comme vous le désirez. Vous devrez donc configurer le navigateur manuellement. Pour cela, allez dans le menu **Outils>Options Internet**. Dans l'onglet **Connexion**, cliquez sur le bouton **Paramètres réseau**. Dans cette nouvelle fenêtre, cochez la case **Utiliser un serveur proxy** et cliquez sur le bouton **Avancé**. Dans la nouvelle fenêtre, remplissez les champs comme sur cette capture d'écran.

POUR TOUS VOS BESOINS, TOUTES VOS ENVIES

LE MEILLEUR DU WEB !

CRACK et KEYGENS

Comment ça marche ?

Même en étant débutant en informatique, vous avez sans doute déjà été confronté aux cracks et aux keygens, ces petits programmes qui permettent d'utiliser un jeu ou un logiciel copié. Comment sont réalisés ces softs, qui les développent, et comment ça marche ?

Crackez moi !

Crée par et pour les hackers, il existe aussi des programmes spécialement conçus pour être craqués. Ils permettent aux crackers de pouvoir s'adonner à leur passion de manière tout à fait légale, pour le fun ou pour se perfectionner. Ces programmes sont appelés des «crackme». Si ce genre de challenge vous intéresse : **http://crackmes.de**

Les cracks «No CD»

Si vous voulez utiliser vote jeu sans avoir à le sortir de la boîte, il existe les cracks «No CD». Comme pour un crack normal, il s'agit la plupart du temps d'un fichier que vous devez placer dans le répertoire du jeu/logiciel. Cette opération changera le fonctionnement du programme : il ne demandera plus l'insertion du CD/DVD !

Mot valise ?

Keygen est un mot-valise pour «key generator» ou générateur de clé en français. Le but de ces programmes est de fournir une clé d'activation valide appelée «serial». Attention, selon la version de votre programme, il faudra un keygen dédié à cette éditon.

Sur les réseaux P2P ou les sites de Warez (ces sites où pullulent les jeux ou programmes piratés), on ne voit que cela : crack, keygen ou NoCD. Il s'agit en fait de programme permettant de jouer ou d'utiliser un logiciel copié. Attention, nous parlons ici de copie et pas de piratage. Il est en effet tout à fait légal de copier un de vos biens pour mettre l'original en sûreté. Voyons comment fonctionnent ces programmes…

Les générateurs de clés

Un keygen est un programme qui a pour but de donner un numéro de série valide d'un simple clic ! La plupart du temps, les auteurs agrémentent leur création d'une musique d'intro ou d'animation psychédéliques pour revendiquer leur acte (comme au bon vieux temps des «trainers» de l'Atari ST). Pour pouvoir donner un numéro valide à chaque coup, les auteurs trouvent l'algorithme utilisé par la société éditrice en désassemblant le code de l'exécutable. Par rétro ingénierie, ils retrouvent le modus operandi permettant de générer un code valide. La méthode «brute force», qui consiste à casser l'algorithme, est devenue très difficile à utiliser vu le grand nombre de caractères qui composent actuellement les clés d'activation des logiciels. De plus en plus, les éditeurs contrent cette méthode en demandant une activation par Internet. Dans ce cas, même si une clé est théoriquement valide, elle sera refusée par le service. Autre technique des éditeurs : bloquer certaines «plages» de clés. Mais cette mesure n'est jamais efficace très longtemps…

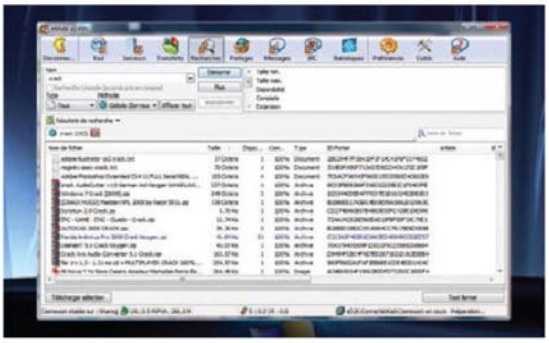
◀ Il suffit de cliquer sur un bouton pour générer une clé d'activation valide !

PRATIQUE ▸

Un crack à la maison

1 Trouver son crack

Pas besoin d'être sorti de Saint-Cyr pour trouver un crack sur Internet. Google est votre ami, eMule et BitTorrent également. Attention, certains cracks sont valides pour une seule version. Si votre logiciel est une version 1.1, le crack de la version 0.9 a



toutes les chances de ne pas fonctionner. Pour les jeux, il faudra faire attention à la langue.

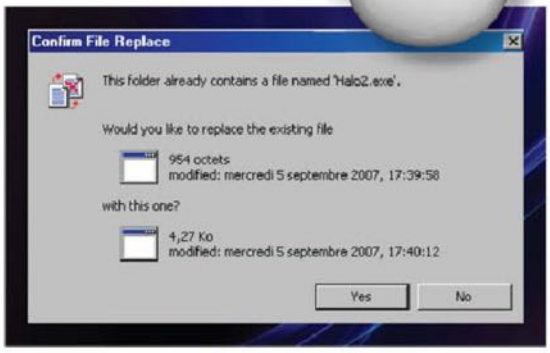
2 Le fonctionnement

Les cracks ne marchent pas tous de la même manière. Dans le dossier compressé où il se trouve, vous trouverez forcément un fichier

.txt expliquant comment utiliser votre crack. Lisez-le avant toute chose. Il faut savoir que la langue utilisée est souvent l'anglais.

3 La substitution

La plupart du temps, le crack est un simple fichier à remplacer dans le répertoire de votre jeu (le plus souvent un fichier **.exe**).



Faites un copier-déplacer puis validez lorsque Windows vous adressera un avertissement de remplacement. Après avoir redémarré votre PC, vous pourrez utiliser votre programme comme si c'était l'original !

Et «crack» la protection !

Les cracks fonctionnent d'une manière différente. La plupart du temps il s'agit d'un fichier «trafiqué» qui va prendre la place d'un fichier similaire dans le dossier d'installation du logiciel/jeu. Il s'agit ici de faire croire au PC que tout va bien et qu'il peut démarrer le programme. Ils peuvent faire croire à l'ordinateur que la clé est bonne (vous pourrez taper n'importe quels caractères), que le DVD est bien dans le lecteur ou que la protection anticopie est bien active. Sur les réseaux P2P, le crack est souvent fourni avec le jeu et est précédé d'une petite séquence présentant le cracker et son groupe. Pour ces individus, il s'agit plus d'une sorte de challenge que d'anarchisme).

Votre clavier SOUS SURVEILLANCE

Plus rarement appelé «enregistreurs de frappe», les keyloggers sont des dispositifs qui permettent d'enregistrer tout ce que vous tapez au clavier. Le but est bien sûr de surveiller l'activité d'un ordinateur. Voyons comment les détecter et les utiliser...

Un keylogger dans la mafia

Dans leur lutte contre le crime organisé, le FBI utilise aussi des keyloggers. En 2002, les collègues de Mulder et Scully ont placé un keylogger matériel sur l'ordinateur d'un membre d'une famille du crime organisé. À l'inverse des écoutes téléphoniques, le FBI n'a pas besoin d'une autorisation pour enregistrer les frappes sur le clavier d'un ordinateur.

À quoi ça ressemble ?

Les keyloggers «matériels» sont de petits dispositifs placés entre la prise du clavier et l'ordinateur. Ils ressemblent à un adaptateur mais attention, ils enregistrent tout sur une mémoire interne. Ce type de dongle est assez rare. Faites attention si vous surfez d'un cybercafé, par exemple... Il existe aussi des claviers avec keylogger intégré !

Les keyloggers ont pour fonction d'enregistrer dans le plus grand secret tout ce que vous tapez sur un clavier d'ordinateur pour transmettre ces données, via Internet, à la personne qui l'a placé sur votre PC. On peut facilement deviner pourquoi un individu ferait une telle chose : récupérer des mots de passe, espionner vos emails (et ce, même si vous utilisez un logiciel de cryptage !), surveiller vos recherches sur Internet, etc. Certains keyloggers plus aboutis permettent aussi d'enregistrer le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application. Les claviers virtuels qu'utilisent les banques en ligne, par exemple, sont donc obsolètes puisqu'un keylogger peut même créer une vidéo qui enregistrerait toute l'activité de votre bureau. Un véritable fléau puisque votre compte bancaire, Paypal, eBay ou votre webmail ne sont plus à l'abri ! Il existe deux types bien distincts de keylogger. Les premiers keykoggers «matériel» (lire lire ci contre) sont assez rares mais vicieux puisqu'aucune parade logiciel n'est possible. En effet, le dongle est invisible et les antispywares passeront à côté bien sûr… La seule solution : être prudent et débrancher tout appareil ou périphérique suspect !

Les keyloggers «logiciels»

Mais les keyloggers les plus répandus sont ceux qui prennent la forme de logiciel. Rien à voir avec un espionnage ciblé puisque la plupart du temps les victimes sont contaminées via un malware (trojan, ver, etc.) contracté par Internet. Ils ne nécessitent donc pas un accès physique à la machine pour la récupération des données collectées. À l'inverse de leurs équivalents «matériels», ces keyloggers ne sont pas limités par la taille de leur mémoire puisqu'ils utilisent le disque dur de leur victime. Ils peuvent donc enregistrer beaucoup plus de choses (captures d'écrans, vidéos, listes de contacts, etc.) Il faut donc être particulièrement vigilant lorsque vous utilisez un ordinateur qui n'est pas le vôtre (école, bibliothèque, cybercafé, etc.)

PRATIQUE ▸

Surveillez votre ordinateur avec KGB Free Keylogger

1 Téléchargement

Si vous désirez la dernière version du logiciel (obligatoirement payante), rendez-vous sur **www.refog.fr/keylogger.html.** Nous vous conseillons néanmoins de faire une rapide recherche sur Google pour trouver un site qui propose **KGB Free Keylogger**, l'ancienne version du logiciel, toujours gratuite !

2 La surveillance

Pendant l'installation, le logiciel vous demandera de choisir la langue (anglais, par défaut) ainsi que le type de surveillance que vous voulez opérer : **Keystrokes typed** (touche de clavier), **Website visited** (les sites Internet), **Program Activity**, **Computer Activity**, etc.

3 Invisible ?

Notez qu'une icône apparaîtra forcément dans le systray (les icônes à côté de l'horloge, en bas à droite). Il est possible de la masquer en faisant un clic droit et en sélectionnant **Hide**. Pour faire revenir le logiciel,

il faudra appuyer simultanément sur **Ctrl** + **Alt** + **Maj** (ou **Shift**) + **K**. Cette version gratuite suffit pour surveiller ce que font vos enfants. Seuls les keyloggers payants offrent une discrétion à toute épreuve.

4 L'interface

Sur le panneau principal, en cliquant dans la colonne de gauche sur **Keystrokes Typed**, vous aurez accès à tout ce qui a été tapé (sélectionnez le logiciel sur la droite). Dans **Clipboard**, il est possible de regarder tous les copier-coller, etc. Cliquez

sur le balai en haut pour nettoyer ce que vous avez déjà vu. Attention, KGB n'est pas tout à fait transparent puisque le logiciel apparaît parmi les logiciels installés.

CE QU'IL VOUS FAUT

> **KGB Free Keylogger** (gratuit)
> **Refog Keylogger** (payant)
www.refog.fr

DIFFICULTÉ

Comment repérer un keylogger ?

Solution 1 : Avant de dépenser de l'argent dans un logiciel, rien ne vous empêche d'essayer de scanner votre PC avec **Spybot Search & Destroy**. Si vous êtes sûr d'être infecté mais qu'aucun logiciel ne détecte votre problème, il va falloir passer à la vitesse supérieure !

Solution 2 : Car les keyloggers passent parfois entre les mailles des antivirus ou des antispywares. Le trojan responsable de l'infection est éliminé mais pas le keylogger qui reste actif. Pour être sûr d'éradiquer toute présence d'un enregistreur, il va falloir utiliser un logiciel spécialisé comme **Anti Keylogger Shield** (30 €).

Solution 3: Vous pouvez aussi surveiller toutes les modifications de fichiers effectuées par les programmes. Si un logiciel agit de manière louche ou si votre base de registre a connu des modifications, vous le saurez ! Il existe plusieurs solutions telles que **Snapshot Spy Pro** et **ArkoSoft System Snapshot** (gratuit).

Jailbreak : LIBÉREZ L'IPHONE !

On entend parler de cette technique un peu partout : au bureau, dans les cours de récré et même dans les médias «généralistes». Le jailbreak consiste en fait à outrepasser les restrictions du système d'exploitation maison d'Apple. A vous la personnalisation des icônes, l'installation de logiciels non agréés ou de véritables transferts de fichiers via Bluetooth...

A la rédaction nous n'aimons pas trop les appareils «figés». Inutile de préciser que les produits Apple font parti du lot : impossibilité de paramétrer comme on le désire, de bidouiller la bête ou même d'installer des logiciels qui n'ont pas été «signés» par la maison mère. Heureusement, le Jailbreaking vient un peu égayer tout ça et puisque c'est légal, pourquoi ne pas tenter l'expérience ?

Jail quoi ?

Le jailbreaking consiste en fait à casser (break) la prison (jail) construite autour de l'iPhone. Et puisque la politique d'Apple est la même pour toute ses productions, il est aussi possible de «jailbreaker» les iPod Touch (incroyable que ça s'achète ce truc non ?) et les iPad (et celui-là alors ?). Il s'agit en fait de hacker l'OS de la machine pour accéder à des fonctions et programmes qu'Apple n'autorise pas à l'origine. Il est par exemple possible de changer le thème, d'installer des logiciels que ne vienne pas forcément de l'AppStore, d'utiliser le

Jailbreak facile !

Depuis la légalisation du déblocage des téléphones par les États-Unis, les choses semblent s'accélérer du côté des logiciels de jailbreaking. Dorénavant, il existe même un service uniquement disponible en ligne. Compatible avec les appareils tournant sous iOS 4 (iPhone, iPad et iPod Touch), JailBreakMe ne nécessite pas d'ordinateur pour procéder à cette manipulation (qui consiste entre autre à pouvoir installer des applications non signées). Il suffit de se connecter à **www.jailbreakme.com** depuis son téléphone. Comme son grand frère, JailBreakMe exploite une faille d'iOS par l'intermédiaire du navigateur Safari. Attention, si vous tentez une telle opération veillez à bien sauvegarder vos données...

www.jailbreakme.com

Encore plus fort ?

La Dev-Team frappe encore ! L'équipe de hackers à l'origine de la découverte du jailbreak mis le doigt sur une faille dans le bootrom (une sorte de BIOS) des iPhone tournant sous iOS 4.1. Rappelons que pour l'instant, Apple se contente de mettre à jour les machines à distance pour réinitialiser leur produit. Non seulement Apple serait d'en l'impossibilité de le faire à l'avenir (à moins de changer le bootrom sur les nouveaux modèles) mais les modifications que pourraient faire les utilisateurs seraient encore plus poussées.

http://blog.iphone-dev.org

PRATIQUE ▸ «Jailbreakez» votre iPhone, iPad ou iPod Touch !

Nous avons vu que pour les iPhone, iPad et iPod Touch sous iOS 4, il suffisait de se connecter avec votre machine au site www.jailbreakme.com et se laisser guider pour jailbreaker votre appareil. En réalité, tous les appareils avant la version 4.0.1 (inclus) sont compatibles avec cette méthode sauf les iPhone EDGE (les premiers, appelés aussi V1). Voyons comment faire...

1 Y'a comme un OS

Attention, si votre téléphone est actuellement jailbreaké et que vous avez déjà l'iOS 4.0 ou 4.01, éviter de faire une mise à jour vers le nouveau 4.1 ! Non seulement vous perdrez totalement votre jailbreak mais vous ne serez pas en mesure d'en faire un autre avant que les équipes de hackers Dev-Team ou Comex ne trouvent une solution pour ce nouvel OS... Si vous n'êtes pas encore passé au 4.0 ou au 4.0.1, c'est le moment ou jamais par contre puisque le site ne fonctionne qu'avec ces derniers.

2 Plus simple tu meurs...

Rendez-vous sur **http://jailbreakme.com** à partir de votre iPhone 3G, 3GS ou 4. Une fois sur le site, glissez la barre **Slide to jailbreak**. Il ne vous reste qu'à attendre pendant le chargement. Une fois que le processus est terminé vous verrez un message vous indiquant que le marché Cydia a été ajouté à votre bureau. De là vous pourrez avoir accès à de nouvelles applications. Votre téléphone est jailbreaké ! Un nouveau monde s'ouvre à vous...

Bluetooth pour transférer ses fichiers et se connecter à un GPS externe. Il est aussi possible d'utiliser son iPhone comme une unité de stockage sans passer par un logiciel payant ou émuler des consoles de jeux (Game Boy Advance, NES, N64, etc.) Il existe même des plates-formes dissidentes comme Cydia, Icy ou Rock qui proposent des milliers de logiciels se passant de l'approbation d'Apple (en effet, les développeurs sont soumis à des règles très strictes concernant l'utilisation de la batterie ou le look de leur création).

Pirate ?

Le fait de pouvoir installer n'importe quel logiciel a bien sûr ouvert la boîte de Pandore puisqu'il est maintenant possible d'utiliser des copies pirates des logiciels officiels d'Apple ou autre. Les réseaux P2P contribuant largement à la propagation des logiciels contrefaits. Attention puisque s'il n'est pas interdit de jailbreaker (une Cour de justice américaine a récemment tranché en faveur des consommateurs et même la Bibliothèque du Congrès des États-Unis encourage cette manipulation), il est bien sûr interdit d'utiliser cette manipulation pour voler les auteurs d'applications. Pour Apple, qu'il soit pour pirater des programmes ou non, le jailbreaking n'est pas autorisé. Selon le constructeur, *«ces techniques, largement généralisées, font appel à des modifications non autorisées du chargeur d'amorçage et du système d'exploitation, ce qui conduit à une violation de notre copyright»*. En effet, les logiciels qui permettent ce jailbreak (QuickPwn ou Pwnage) contiennent des pans de code qui appartienne à la société et qui sont en plus bidouillé sans son consentement bien sûr. Apple a donc décrété que l'opération empêchera la garantie de fonctionner. Pourquoi ? Parce que le jailbreak est susceptible de compromettre la sécurité de l'iPhone. Mouais, c'est de bonne guerre… Apple combat dorénavant cette tendance en mettant à jour la machine car à chaque fois, le jailbreaking est à refaire (bien sûr il faudra sauvegarder vos applications achetées sur Cydia ou autre). Heureusement que cette opération n'est pas bien compliquée…

CE QU'IL VOUS FAUT

> **Jail Break Me** (gratuit)

www.jailbreakme.com

DIFFICULTÉ

Retrouvez des fichiers EFFACÉS

Une fois un fichier ou un dossier supprimé de la corbeille, la plupart des utilisateurs pensent avoir effacé définitivement ces éléments. C'est faux. Des logiciels existent pour ressusciter ces données qui laissent toujours des traces de leur existence passée...

Lorsque vous effacez un fichier (de la corbeille ou directement d'une carte mémoire, par exemple) ce dernier ne disparaît pas complètement. Le système «l'oublie» mais ne l'effacera que si un autre fichier est enregistré au même endroit. Si vous venez juste de commettre votre erreur, vous pouvez encore la rattraper. Il existe en effet des logiciels qui vont retrouver les fragments de fichier et les reconstituer si possible. Le mieux est d'installer ce type de logiciel avant d'avoir à récupérer un fichier : on ne sait jamais, peut-être que l'installation endommagera votre précieuse photo ou vidéo encore conservée dans les méandres de votre disque dur.

CE QU'IL VOUS FAUT

> Recuva file recovery (gratuit)
www.recuva.com

DIFFICULTÉ

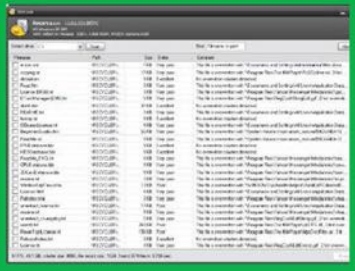
Effacer efficacement ?

Si vous ne voulez pas qu'on utilise Recuva ou un autre logiciel de ce type contre vous (pour retrouver des fichiers sensibles dans votre disque dur), il existe une parade ! Le logiciel Eraser vous permet d'effacer complètement un dossier, un groupe de fichier ou une partition. Pour cela, il ira jusqu'à réécrire 35 fois par-dessus ce que vous voulez supprimer (voir notre microfiche n° 5 page 43) !

PRATIQUE ▶ Recuva, un vrai jeu d'enfant !

1 La recherche

Après installation, l'assistant va vous demander quel est le type de fichier que vous voulez récupérer (musique, documents, etc.) puis le dernier emplacement connu (**Mes Documents**, **Corbeille**, carte Flash, etc.)



Enfin vous pouvez cocher la case **Analyse approfondie** qui permet de rechercher avec plus de perspicacité. Validez et laissez le logiciel faire son travail.

2 L'indice de confiance

À la fin du scan, Recuva va afficher les noms des fichiers, leur emplacement et leur **Etat**. Une pastille verte signifie que le fichier est encore en bon état et peut être récupéré alors qu'une pastille orange permet une récupération partielle (si c'est une vidéo, il sera difficile d'obtenir un bon résultat). Par contre, avec une pastille rouge, la restauration est impossible, vous avez attendu trop longtemps ou vous avez opéré trop de changement sur votre disque dur.

3 Dernières choses...

Notez que Recuva permet aussi de restaurer des dossiers qui ont été supprimés par des bugs, des accidents et des virus. Si vous avez perdu un fichier temporaire de Microsoft Office (durant une panne de courant), Recuva peut aussi vous sauver la mise...

ZIP, XLS, PDF : HACKEZ-LES TOUS !

Avant de jeter à la corbeille ce fichier ZIP dont vous avez oublié le mot de passe, ce classeur Excel protégé par un collègue trop zélé (et donc viré depuis 3 mois) ou ce PDF malencontreusement verrouillé, jetez d'abord un coup d'œil à cet article. Avec certains logiciels ou manipulations, il est possible d'avoir accès à des fichiers que l'on pensait condamnés...

CE QU'IL VOUS FAUT

> ZIP Password Finder (gratuit)
www.astonsoft.com
> PDFPassword Remover (gratuit)
www.verypdf.com

DIFFICULTÉ

PRATIQUE ▸ ZIP Password Finder

Astonsoft ZIP Password Finder est un logiciel qui va cracker la protection des fichiers ZIP verrouillé par mot de passe. La méthode utilisée est la «brute force» qui va essayer tous les mots de passe jusqu'à obtenir le bon. L'utilisateur a simplement à spécifier le nombre de caractères du mot de passe et le type de caractères utilisés (chiffres, minuscules, majuscules, etc.) pour que débute la recherche. Attention, si un mot de passe de 10 chiffres ne prend pas plus d'une demie journée à décrypter, un mot de passe composé de plusieurs types de caractère prendra quelques dizaines d'années... ZIP Password Finder est moins complet et moins puissant que son concurrent Advanced ZIP Password Recovery (qui permet aussi de cracker d'autres types d'archives) mais gratuit : **www.elcomsoft.com/azpr.html**

1 Les types de caractères

Après l'installation du logiciel, lancez-le et cliquez sur **Open file** et chargez le fichier ZIP que vous voulez cracker. Dans la colonne de gauche, sélectionnez le type de caractères que vous avez utilisé lors de la saisie (si vous vous souvenez !).

2 Patience...

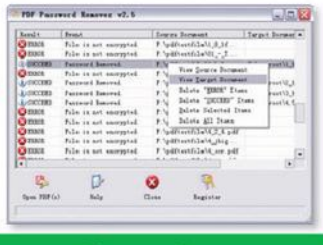
Il est possible de ne choisir qu'un type de caractère pour parvenir plus facilement à vos fins. Dans la colonne de droite, saisissez le nombre maximum de caractère en face de **Max Password Length**. Cliquez sur **Start** en haut à gauche. Il ne reste qu'à vous armer de patience...

PRATIQUE ▸ PDF Password Remover

PDF Password Remover permet de déverrouiller les fichiers PDF protégés par un mot de passe. Ces protections, très pratiques lorsque vous voulez éviter de vous faire voler le contenu d'un document, peuvent se retourner contre vous si vous oubliez le mot de passe ! Le logiciel que nous vous proposons permet de récupérer tous les droits sur le PDF : modification, impression, édition des Acroforms, récupération des images, etc. Il supporte le glisser-déposer, le décryptage 40-bit RC4, 128-bit RC4, AES, les fichiers compressés et les Metadatas non cryptés. Attention, cette version, d'essai ne décrypte que la première moitié de la première page. Si vous êtes satisfait du résultat, il faudra passer à la caisse ou utiliser ce service en ligne : **www.pdfunlock.com**

1 Facile !

Cliquer sur **Open PDF(s)** pour sélectionner plusieurs fichiers, soit vous pouvez effectuer un glisser-déplacer sur la grille. Une fois sélectionné, une fenêtre apparaît pour vous demander le répertoire de sortie. Cliquez sur **OK**. Vous avez maintenant accès à toutes les fonctions sur votre fichier PDF (sélection, édition, copie, etc.)



2 Version «ligne de commande»

Si vous avez ce message d'erreur, c'est que le fichier n'est pas protégé. Il existe aussi une version ligne de commande (pour effectuer des scripts par exemple), il suffit de lancer le fichier **pdfdecrypt.exe**.

Pour les fichiers Excel aussi ?

Pour finir, voilà une petite astuce qui va vous permettre de faire sauter rapidement la protection d'un classeur ou d'une feuille Excel. Pour ce faire, il va falloir utiliser une macro. Ouvrez le fichier que vous voulez cracker et sélectionnez **Outils > Macro > Visual Basic Editor**. Allez ensuite sur cette page (**www.vbfrance.com/codes/OTER-PROTECTION-FEUILLES-CLASSEUR-EXCEL-METHODE-SANS-ECHEC_36857.aspx**) et faites une copie du code de la ligne 49 à la fin de la ligne 165. Collez cette partie dans le Visual Basic Editor puis sauvegarder vos modifications. Sélectionnez alors Outils > Macro >Macros puis exécutez la macro Deproteger. Après quelques instants, le mot de passe qui protégeait la feuille Excel devrait s'afficher ! Cette manipulation fonctionne avec Excel 97, 2002 et peut-être d'autres...

Attaques DDoS : «Nous sommes légion»

Un groupe de hackers nommé Anonymous a déclaré la guerre aux défenseurs des ayants droit. Avec un logiciel spécial, un peu d'organisation et des milliers de sympathisants, ils ont lancé des attaques de déni de service sur les sites de la MPAA et de la RIAA rendant ces derniers inopérants jusqu'au lendemain. Explication sur ce phénomène et son fonctionnement...

L'opération Payback a commencé le 19 septembre dernier et la lutte ne fait que commencer. Il s'agit en fait d'une attaque DDoS (pour Distributed Denial of Service ou «déni de service» en français) visant à saturer de requête des sites pour qu'il ne soit plus en mesure de répondre. Le but est bien entendu de rendre la monnaie de sa pièce aux majors et à ceux qui les protègent. Après la MPAA (Motion Picture Association of America), la RIAA (Recording Industry Association of America et la société indienne AirPlex Software (qui essaye de faire tomber les trackers comme ThePirateBay avec… des attaques DDoS !), Anonymous parle d'attaquer notre HADOPI national ! On parle aussi de Trident Media Guard, la société qui scrute le Net à la recherche de contrevenant pour le compte de la haute autorité.

Le logiciel LOIC

L'originalité de Payback réside dans son système d'attaque. Au lieu de s'en prendre à un serveur avec une

La loi ?

Attention même si ce petit jeu peut sembler amusant, en France *«Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.»* Dans les faits, seuls les instigateurs pourront éventuellement être inquiétés...

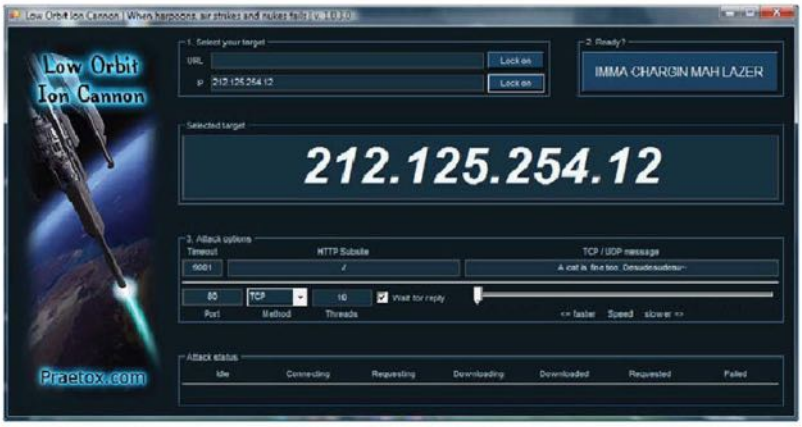
Pas très sport

Avec l'augmentation des échanges commerciaux sur Internet, le nombre de «chantages au déni de service» est apparu. Il s'agit pour un pirate de lancer une attaque DDoS contre une entreprise et de lui demander une rançon pour la faire cesser. En 2008, trois pirates russes ont écopé de 8 ans de prison suite à un chantage envers des sites de jeux en ligne.

Vous avez dit «zombie»

Pour contrer les pirates, les entreprises qui pourraient perdre énormément d'argent si leur site restait inactif placent des protections coûteuses au niveau de leurs serveurs. Devant la quantité toujours plus importante de participant nécessaire, certains pirates n'hésitent pas à faire appel à des légions de «PC zombie». Des ordinateurs contaminés par un trojan qui peuvent envoyer des requêtes vers la cible sans que le propriétaire s'en aperçoive...

seule machine ou une grosse quantité de PC «zombie», le groupe de hackers a préféré se bâtir une petite communauté de «soldats». Et pour que chacun puisse prendre part à l'attaque Anonymous met à disposition un programme répondant au doux nom de LOIC (comme le «Low Orbit Ion Cannon» de L'Empire contre-attaque). Pour utiliser ce logiciel, pas la peine d'être un pro de la sécurité informatique ou un pirate aguerri, il suffit de rentrer une adresse IP et de cliquer sur un bouton à l'heure du «rendez-vous». Même l'interface n'a rien à voir avec les logiciels de ce type : mode graphique, design soigné, etc. Il est d'ailleurs intéressant de noter que ce type de logiciel, même sans l'artillerie lourde que doivent posséder Anonymous est opérationnel pour n'importe quel site. Les FAI complices d'HADOPI pourraient très bien voir leur activité freinée par LOIC. Pas la peine non plus de chercher bien loin puisque LOIC est disponible sur le site SourceForge, une grosse base de logiciels libres tout à fait «fréquentables»...



L'organisation

Organisé de longue date sur différents réseaux (comme le forum 4chan.org, rockstararmy.com, Usenet, etc.) et même Twitter (http://twitter.com/savetpb), ce phénomène a connu un énorme succès et les internautes intéressés se passent le mot par le bouche-à-oreille. C'est ainsi que le 7 octobre dernier nous avons été témoins d'une attaque sur le site www.sgae.es (Sociedad General de Autores y Editores, une sorte de SACEM espagnole). En moins de 10 minutes, le site était rendu inopérant. Il n'est pas possible de savoir combien d'internautes ont été complice de cette attaque mais il faut reconnaître qu'elle a été diablement efficace. Le site de la SGAE a été gelé jusqu'au lendemain. Anonymous, ne cache pas sa sympathie pour The Pirate Bay, qui a en effet connu de nombreux problèmes d'accès ces derniers temps. Les pirates répondent donc avec les mêmes armes que les ayants droit. Ce type d'attaque étant difficilement évitables, les sites les subissant ne peuvent qu'attendre que l'orage passe. Il est très fréquent que le site ne soit pas disponible immédiatement après, le retour aux conditions normales peut exiger une intervention humaine. C'est pour cela que les effets peuvent se prolonger pendant plusieurs heures. Relativisons aussi la gravité de ces actes qui ne sont pas réellement pénalisants pour ces sociétés. En effet, rendre indisponible les sites de la MPAA ou de la RIAA n'a rien de dramatique. Mais attention, les hackers pourrait passer à la vitesse supérieure en choisissant de cibler des sociétés beaucoup plus dépendantes de leur site Internet. Ce n'est bien entendu pas la même chanson s'il s'agit d'un site commercial. Mais le groupe ne compte pas en rester là puisque les hackers visent à se créer un véritable réseau d'individus qui permettrait d'attaquer quiconque s'en prendrait à la neutralité du Net. Anonymous évoque également la possibilité de «spammer le fax» et de «saturer le standard téléphonique» de cabinets d'avocats.

◀ Ce flyer trouvé sur le net propose d'attaquer le site de la BPI (British Phonographic Industry) le 20 septembre à 4h GMT. Accusé d'être complice dans la kabbale lancée contre ThePirateBay, la consigne est claire : armez vos lasers et faites feu !

▲ La simplicité du logiciel LOIC permet à des milliers de newbies de participer aux attaques

CE QU'IL VOUS FAUT

> Low Orbit Ion Cannon (gratuit)
http://sourceforge.net/projects/loic/files

DIFFICULTÉ

Qui en veut à votre Wi-Fi ?

On savait déjà que les clés WEP ne protégeaient pas assez les connexions Wi-Fi, c'est aujourd'hui, la clé WPA, considérée jusqu'ici comme inviolable, qui est mise à mal par des chercheurs. A l'heure où il s'avère de plus en plus facile de pirater une connexion, comment monsieur «Tout le monde» peut-il se protéger ?

Cracker le Wi-Fi c'est facile. Devenir un pirate est à la portée de tous. Pour s'en convaincre, il suffit de taper «cracker» et «Wi-Fi» dans Google pour tomber sur un site proposant de «tester» la sécurité de votre système. Il s'agit ni plus ni moins que de méthodes permettant de pirater n'importe quelle connexion, même si les auteurs s'en défendent. Ces sites se sont longtemps épanchés sur la fragilité de la clé WEP (Wired Equivalent Privacy), censée fournir une sécurité équivalente aux câbles. Ce système de cryptage des ondes est pourtant utilisé par défaut par de nombreuses box grand public. Alors que de plus en plus de pirates amateurs s'essayaient avec succès au décryptage de clés WEP, les fournisseurs d'accès comme les professionnels du secteur, recommandaient de passer à un cryptage supérieur, le WPA qui signifie, Wi-Fi Protected Access. Un programme alléchant qui a titillé l'esprit de nombreux chercheurs. Deux d'entre eux, Erick Tews et Martin Beck, ont réussi

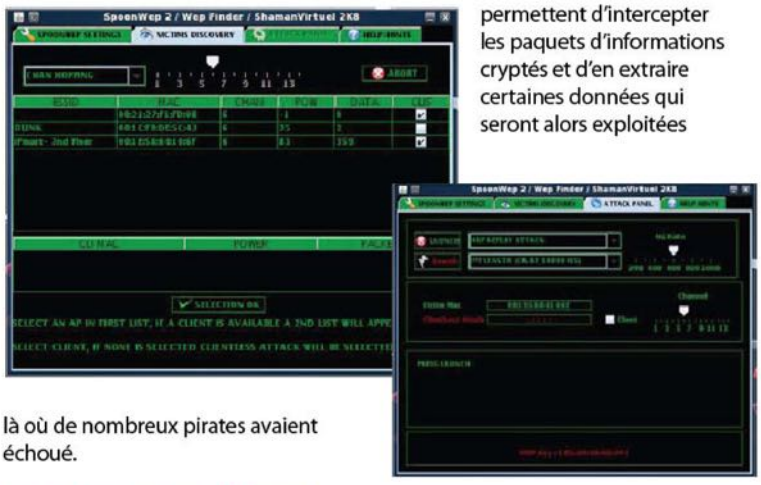
Piraté et coupable !

Si la clé WPA2 est encore considérée comme fiable (tout comme la WPA-PSK), il s'avère qu'elle n'est pas configurée par défaut sur les appareils grand public. Il est difficile pour les utilisateurs lambda de reconfigurer manuellement leurs routeurs. On peut facilement imaginer que la «Loi internet et création» forcera les adeptes du téléchargement illégal à pirater les lignes peu protégées. Un internaute qui se fera pirater sera alors considéré comme coupable et se verra condamné. Cette simple hypothèse démontre un peu plus, s'il était nécessaire, l'aspect irrationnel d'HADOPI et compagnie.

Un hack clé en main

Alors que le piratage du Wi-Fi du voisin était encore un sport réservé à l'élite, une société malaisienne propose un pack regroupant un adaptateur Wi-Fi et une distribution Linux spécialisée dans la sécurité réseau (BackTrack). Appelé WiFi Box, cette dernière permet de cracker les clé WEP et WPA en quelques minutes...

http://wifi-box.com



permettent d'intercepter les paquets d'informations cryptés et d'en extraire certaines données qui seront alors exploitées pour déverrouiller la clé. Ces logiciels sont disponibles gratuitement avec des distributions Linux, telles que Backtrack. Il existe des «Live» CD qui permettent de faire tourner Linux dans un PC sous Windows sans installation. Une manipulation très simple, qui ne nécessite pas de connaissances poussées. Une fois la distribution installée, il suffit de lancer les programmes suivants, Airmon, Airodump et Aireplay. Ces logiciels libres ont déjà été mis à jour et équipés de l'algorithme d'Erick et Martin. Ils sont donc potentiellement capables de décrypter un chiffrage WPA...

là où de nombreux pirates avaient échoué.

Les chercheurs gagnent du temps

Jusqu'à présent, la méthode utilisée pour casser les clés WPA consistait à tester toutes les combinaisons possibles. Cette technique longue et fastidieuse est aussi connue sous le nom de force brute. C'est là que Erick et Martin innovent. Ils ont trouvé un moyen de décrypter ce type de clé en seulement 15 minutes. Leur méthode consiste à envoyer un maximum d'information au routeur le forçant à révéler des informations sur la clé de cryptage. Les chercheurs ont récemment présenté leur trouvaille au forum de PacSec au Japon, sous les regards médusés des plus grands spécialistes de la sécurité informatique.

Comment ça marche ?

Les ondes Wi-Fi, à l'instar des ondes radios, se baladent partout autour du point d'émission, hotspot ou routeur Wi-Fi. Certains logiciels

C'est grave docteur ?

Mais est-ce si grave de se faire pirater sa connexion ? A part le débit qui en prend un coup, ce n'est pourtant pas la mer à boire me direz-vous...

Certaines personnes ne s'en rendent même pas compte lorsqu'ils ont un squatter sur les WiFi. Le problème, c'est qu'en plus de se faire pirater le contenu de son ordinateur, vous devenez responsable de ce que votre squatter consulte et télécharge ! En effet, la loi Hadopi réinvente le délit de négligence, autrement dit, si vous ne protégez pas votre accès Wi-Fi, vous serez condamnables. Si les

3 trucs pour verrouiller votre connexion

1 > Le filtrage d'adresse MAC

Une adresse MAC est la carte d'identité physique de votre ordinateur, elle lui est propre. En configurant votre routeur, vous pouvez autoriser seulement les adresses MAC que vous désirez. Si cette méthode n'arrête pas les pirates les plus aguerris, elle découragera les moins téméraires.

2 > La clé WPA2

Basée sur le cryptage WPA, elle possède une couche de protection supplémentaire avec un cryptage AES, réputé inviolable. Utilisez une chaîne de caractères assez longue et variée. Changez de mot de passe fréquemment et vous devriez être tranquille.

3 > Cacher votre identité

Le SSID (Service Set Identifier) est le nom de votre connexion. Il sert à identifier votre point d'accès, les box le génèrent automatiquement. En le dissimulant, vous compliquerez considérablement la tâche des pirates en herbe.

CE QU'IL VOUS FAUT

> Airsnare (gratuit)

http://home.comcast.net/~jay.deboer/airsnare/Index.html

DIFFICULTÉ

spécifications officielles se font désirer, mieux vaut prendre les devant. Alors comment savoir si quelqu'un utilise votre ligne ? C'est très simple, il suffit d'installer le logiciel AirSnare.

À ne pas mettre entre toutes les mains !

Il s'agit d'un outil gratuit permettant de détecter les ordinateurs non autorisés sur votre connexion. Il surveille les adresses MAC (adresses physiques propres à chaque ordinateur), plus difficilement falsifiables que les adresses IP. Lorsqu'un nouvel utilisateur essaie de se connecter à votre réseau, celui-ci fait une requête (DHCP) pour obtenir une adresse. Ces requêtes sont également surveillées. AirSnare est un logiciel puissant fournissant de nombreuses informations confidentielles à ceux qui l'utilisent. Attention donc à ne pas franchir la barrière et tomber dans le camp des pirates !

Obtenir l'IP des malotrus

Une fois que vous avez détecté un intrus avec AirSnare, vous pouvez le pister, et comme on dit dans le jargon, sniffer toutes les informations qu'il émet sur le réseau. Pour cela, vous aurez besoin d'un logiciel complémentaire, Wireshark. Ce logiciel analyse les paquets d'informations circulant sur le réseau et en affiche les détails. Attention, certains mots de passe peuvent apparaître en clair.

PRATIQUE ▶

Espionnez les espions !

1 Installation

Une fois téléchargé, AirSnare s'installe de façon relativement classique. Sous certaines versions de Windows, il se peut que vous ayez à installer un composant supplémentaire, la librairie **WinPcap**. Vous

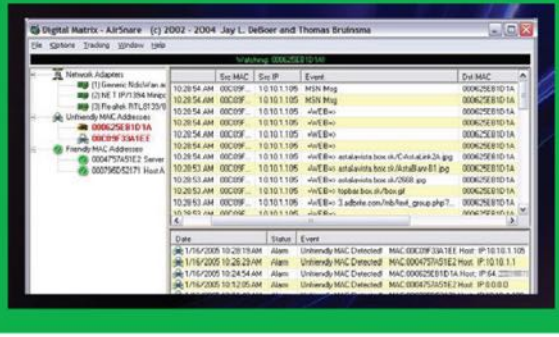
la trouverez ici : **http://winpcap.polito.it** sous l'onglet **Tools**. Notez que cette librairie est incluse dans **Wireshark**, la meilleure option étant donc d'installer aussi ce logiciel.

2 Configuration

Assurez-vous de bien installer AirSnare sur un ordinateur lié au réseau que vous voulez surveiller. Si vous souhaitez voir qui se connecte à la box, il est important que le SSID de votre ordinateur soit identique. Le SSID n'est autre que le nom de votre Wi-Fi. Votre logiciel est maintenant installé. Démarrez-le et sélectionnez votre carte réseau dans la liste sur la gauche. Votre carte Wi-Fi devrait comporter l'indication 802.11, ceci vous permettra de la reconnaître.

3 Surveillance

Maintenant que tout est paramétré, lancez la surveillance de votre réseau en cliquant sur le bouton **Start**. Les adresses autorisées seront cataloguées dans la partie **Friendly MAC Addresses**, dans la colonne de gauche. En revanche, si certaines adresses sont suspectes, elles seront affichées en rouge dans **Unfriendly MAC Addresses**. Il se peut que votre Xbox ou votre imprimante apparaisse dans la liste non désirée (ce numéro apparaît généralement sur le matériel). Si tel est le cas, faites un clic droit puis choisissez **Add to Trusted**.



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

GO

Antivirus, anti-spyware, protection résidente, etc. Lorsque l'on parle de sécurité, il ne faut pas faire les choses à moitié. Cependant, entre une protection trop faible et trop de protections, il faut parfois viser juste. Voyons quels sont les meilleurs logiciels pour blinder votre PC et comment bien les utiliser...

Blindez VOTRE PC !

Heuristique ?

Les principaux antivirus du marché fonctionnent grâce à des fichiers de signatures. Il s'agit alors de télécharger régulièrement les mises à jour pour que le logiciel compare la signature du virus avec ce qui se passe comme symptôme sur le PC. La protection heuristique, elle, permet de découvrir un code malveillant par son «comportement». Avec cette dernière, de fausses alertes peuvent être provoquées mais les mises à jour ne sont plus nécessaires.

En ligne ?

Si vous êtes sur un ordinateur qui n'est pas le vôtre, il est possible d'avoir accès en ligne à un antivirus qui va le scanner à distance. Vous ne profiterez pas de protection résidente mais pourrez détecter un problème sans avoir besoin d'installer quoique ce soit. BitDefender propose, par exemple, ce genre de service...

www.bitdefender.fr/scanner/online/free.html

> Antivirus

Les antivirus permettent d'identifier et d'éliminer les virus et les malwares de manière générale. Même si certains antivirus gratuits s'occupent aussi bien des spywares, il est préférable de s'équiper aussi d'un anti-spyware. Attention, il ne sert à rien d'installer deux antivirus sur un ordinateur. Ils pourraient se marcher sur les pieds plus que de vous aider. Sachez aussi que de plus en plus d'antivirus proposent une protection résidente. Non seulement, vous disposez d'un module permettant de scanner votre PC si vous soupçonnez une infection mais le logiciel déploie un bouclier qui permet de contrer une attaque au moment où elle survient. Les antivirus payants proposent les mêmes options mais sont beaucoup plus exhaustifs au niveau des fonctionnalités.

LE CHOIX DE LA RÉDACTION

BITDEFENDER > Le top de la protection

BitDefender est connu depuis bien longtemps par les pionniers de la Toile. Même s'il est moins populaire que d'autres solutions gratuites, ce dernier propose toujours une protection ultra-complète pour toutes les utilisations : FTP, P2P, e-mail, messagerie instantanée, stockage externe, etc. De surcroît, BitDefender intègre une protection dite «proactive» permettant de faire le ménage sans avoir nécessairement toutes les signatures de virus en sa possession. Si vous êtes séduit par la version gratuite de BitDefender, participez au concours page 4 pour tenter de gagner BitDefender Internet Security 2011 !

www.bitdefender.fr

> Anti-spyware

À l'inverse des virus ou autres malwares, le spyware se veut discret. Il est là pour vous espionner et transmettre des informations à des tiers : spammer, black hat et autres personnes malintentionnées. Au final, les risques de contamination sont encore plus importants. Raison de plus pour éradiquer ces méchantes petites bêtes... Attention, lorsque vous installez certains logiciels peu recommandables, il arrive que ces derniers vous recommandent une installation complémentaire. Si vous ne connaissez pas ces programmes, évitez de succomber autant que faire se peut...

SPYBOT - SEARCH & DESTROY > L'unique !

Il n'y a pas que les vers et les virus qui peuvent mettre en danger votre PC. Les spywares, ces logiciels espions qui scrutent vos habitudes sur le Net sont aussi à compter parmi les indésirables. Grâce à Spybot, vous faites le grand ménage dans vos fichiers jusque dans la base de registre. À chaque détection, vous aurez le loisir de choisir l'action à accomplir... Nous vous conseillons de faire une sauvegarde de la base de registre avant toute grosse modification.

www.safer-networking.org

> Anti-adware

Les adwares ne cherchent pas à contaminer votre PC mais ils veulent avant tout vous faire perdre la tête ! Si vous avez des publicités incongrues qui s'affichent un peu partout sur votre écran ou si des pages Internet pleines de pub s'ouvrent automatiquement, c'est que vous avez choppé une de ces méchantes bêtes. En plus de ralentir votre bécane, ces publicités sont ennuyeuses au possible. Résistez et installez un anti-adware !

AD-AWARE > Fini la pub !

Ad-Aware est un utilitaire qui vérifie la mémoire, la base de registre et les disques durs afin de détecter les adwares. Ces logiciels, ayant pour but d'afficher de la publicité durant vos surfs, peuvent drastiquement diminuer les capacités de votre ordinateur ; une bonne raison pour ne pas faire de quartier ! Vous pouvez choisir la profondeur de l'examen ou encore la sélection des tests effectués (vérifier uniquement le registre ou les processus actifs, par exemple). L'interface est claire et facile à prendre en main.

www.lavasoft.com/products/ad_aware_free.php

AVAST > Un bon challenger

Avast est un logiciel édité par ALWIL, une société tchèque spécialisée dans la sécurité. La qualité de la version familiale d'Avast n'est pas une surprise quand l'on sait que la société éditrice a fait le choix d'en faire son cheval de bataille. En effet, une version familiale gratuite et de qualité est un gage, pour les professionnels, d'avoir une version payante conforme à leurs attentes.

www.avast.com/fr

HIJACKTHIS > Spécial parano !

Ce logiciel s'adresse à tous ceux qui pensent (à tort ou à raison) être victimes d'attaques en ligne. HijackThis permet de localiser les programmes malintentionnés pour pouvoir ensuite les éliminer. Le logiciel ne nécessite aucune installation : il scanne votre machine puis rend son verdict sous forme de log (ou fichier journal). Il suffit de copier-coller ce log sur le site de l'éditeur pour connaître ses points faibles...

www.hijackthis.de/fr

> Anti-spam

Gentiment appelé «pourriel» par nos amis Québécois (contraction de «pourri» et «courriel»), le spam est un véritable problème depuis le début des années 90. Les principaux acteurs de cette calamité sont des producteurs de produits pharmaceutiques, des diffuseurs de contenu pornographique, des organismes de crédits, etc. Attention le spam permet de «faire passer» des arnaques beaucoup plus redoutables dans vos boîtes aux lettres. Le phishing, par exemple ! Si vous n'avez ni de Webmail (comme Gmail) ni le logiciel Mozilla Thunderbird (qui intègre de puissants antispam), il va falloir vous équiper d'un logiciel spécialisé... C'est tellement plus sympa de lire ses e-mails sans qu'on vous propose du Vi4gr4 toutes les 2 lignes...

SPAMFIGHTER > Un logiciel et une communauté

SPAMfighter Standard est un filtre antispam gratuit fonctionnant pour Outlook, Outlook Express et Windows Mail. Ce logiciel utilise son réseau de plus de 7 millions d'utilisateurs pour éliminer le spam. Dès qu'un utilisateur reçoit un spam,

ce dernier peut l'éliminer à la main si le logiciel ne l'a pas fait. Les serveurs de l'éditeur vérifient l'information et ce spam est placé sur une liste noire : il est ainsi détecté et éliminé chez tous les autres utilisateurs. Ce système très malin permet d'éradiquer presque 100 % des courriers indésirables.

www.spamfighter.com

> Firewall

Les firewall ou pare-feu sont un autre élément indispensable lorsque l'on parle de la sécurité d'un ordinateur. Ils permettent de surveiller les entrées et sorties de votre PC lorsqu'il est connecté à un réseau. Nous revenons sur ces logiciels plus en détail à la page 30 de ce magazine...

On vous ESPIONNE ?

Perte de bande passante, messages d'erreur incompréhensibles ou activité suspecte : c'est parfois le signe d'une intrusion dans votre système. Voyons comment vérifier si quelqu'un se connecte à votre PC et mettre un terme à ses agissements avant qu'un malheur n'arrive...

Vérifiez l'activité en votre absence

Si vous n'êtes pas le seul à utiliser votre ordinateur (ami, enfant, etc.), vous devriez aussi contrôler l'activité sur votre machine. Les sites pornographiques ou de warez sont particulièrement «à risque». Pour cela, vous pouvez installer un keylogger (qui enregistrera les frappes au clavier, voir page 18), verrouiller votre session avec un nouveau mot de passe et vérifier les dernières installations dans **Panneau de configuration > Programmes et fonctionnalités.**

13 millions de PC zombie orphelins

Pendant l'été, le créateur du gigantesque botnet Mariposa (un réseau de PC zombie) a été arrêté ! Fort de 13 millions de machines contaminées, Mariposa a servi à pirater des cartes bancaires et des comptes en ligne de 500 grandes entreprises et 40 banques.

Poutine et Medvedev aussi !

Personne n'est à l'abri d'une intrusion informatique puisque le FSO (chargé de protéger des personnalités russe comme le Premier ministre et le Président) en a été victime. Le système de messagerie n'a pas résisté aux attaques de hackers, qui y ont pénétré le 23 août dernier. Les autorités russes ont minimisé l'impact de cette intrusion informatique mais des archives de courrier étaient disponibles sur Internet pendant plusieurs jours...

Cette fois vous en êtes sûr, quelque chose cloche avec votre PC. Vous n'êtes pas pourtant du genre à installer n'importe quoi ou à ouvrir les fichiers joints d'un fils de ministre Gabonais (qui vend du Viagra pour sauver les derniers dauphins d'eau douce). Pourtant l'activité de votre ordinateur est suspecte : icônes qui bougent toutes seules, logiciels qui ne démarrent plus, bande passante réduite, etc. Bien sûr, votre premier réflexe est de faire un scan complet avec tout l'arsenal mis à votre disposition (antivirus, antispyware, etc.) mais rien n'y fait. Vous en arrivez à l'évidence : quelqu'un utilise votre PC à votre insu, en local ou à distance dans le but de vous espionner ou de vous voler quelque chose…

À l'insu de votre plein gré ?

S'il s'agit de votre PC au travail, vous ne pouvez pas faire grand-chose puisqu'il est évident qu'un administrateur réseau peut techniquement faire et récupérer à peu près ce qu'il veut sur un poste qu'il gère.

Attention cependant, puisque si vous n'avez pas été averti par votre patron, vos documents, activité, journal de connexion ne peuvent pas motiver une quelconque sanction. Cela relèverait du non-respect de la vie privée. Pour son ordinateur personnel, c'est plus préoccupant puisque personne, à part vous, ne s'occupe de la sécurité. Et si votre PC était contrôlé à distance grâce à un logiciel du type Radmin (logiciel de prise de contrôle en ligne) ou un méchant Trojan ? Si votre upload est égal ou supérieur à votre download, attention ! N'oubliez pas que vous êtes responsable devant la loi de ce qui passe par votre machine ! Passez votre souris sur l'icône en forme d'écran en bas à droite à côté de l'horloge pour vérifier ces chiffres. En plus de vérifier que votre pare-feu est bien activé (**Panneau de configuration** > **Centre de sécurité**), il va falloir tester les ports ouverts ou en activité sur votre machine. Connectez-vous au service ShieldsUP! : **www.grc.com**. Cliquez sur **Proceed**, puis sur **All service port**, patientez pour avoir le résultat, toutes les cases doivent être vertes.

En cliquant sur chacune des cases, vous obtiendrez le détail de chaque port (le nom du logiciel qui l'utilise, l'utilisation habituelle, la description, etc.) Vous pouvez aussi tenter le scan en ligne de Microsoft, le Windows Live OneCare. Cliquez sur analyse complète puis lisez attentivement les résultats : **http://onecare.live.com/site/fr-fr/default.htm**. Si certains ports semblent suspects, il faudra les fermer manuellement dans votre pare-feu. Si vous ne constatez rien, peut-être que votre firewall n'est pas si fiable que vous le pensez. Faites ce test pour vérifier son intégrité : **www.grc.com/lt/leaktest.htm**.

◀ **Radmin, qui permet de prendre le contrôle de votre PC à distance, peut être utilisé contre vous !**

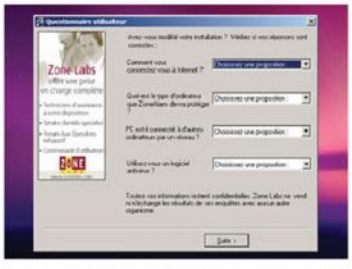
PRATIQUE ▸

Évitez les intrusions avec ZoneAlarm

Si vous n'avez pas de pare-feu (depuis Windows XP SP2, tous les OS de Microsoft en sont équipés par défaut), il serait temps d'en installer un ! Un logiciel de ce type permet de protéger l'accès à votre ordinateur en plaçant une sorte de barrière entre votre machine et Internet.

1 Le formulaire

Pendant l'installation, le logiciel vous demandera de remplir un formulaire ainsi que de répondre à quelques questions (type de connexion, etc.) Après le redémarrage obligatoire, ZoneAlarm va vous proposer deux



versions. Choisissez la gratuite et poursuivez l'installation. Notez que pendant que l'assistant vous guidera, votre connexion Internet sera bloquée. Ne vous inquiétez pas, c'est tout à fait normal.

2 Alerte !

Maintenant que le programme est installé, il va falloir lui dire "d'autoriser" les programmes que nous utilisons pour nous connecter à Internet. La solution la plus simple consiste à valider les programmes les uns après les autres. Si vous ouvrez MSN, par exemple, une fenêtre d'alerte s'affichera.

3 L'autorisation

Cochez la case **Conserver ce paramètre** et cliquez sur **Autoriser**. Maintenant, votre programme fait partie des programmes considérés comme sûrs de ZoneAlarm. Parfois une deuxième alerte s'affiche : Là encore, il faudra autoriser le programme à se connecter à Internet.

4 Le Contrôle

Pour voir les logiciels autorisés à communiquer avec l'extérieur, double-cliquez sur l'icône de ZoneAlarm dans le systray (en bas à droite à côté de l'horloge). Cliquez ensuite sur **Contrôle des programmes**, puis allez dans l'onglet **Programmes**. Si vous voyez un logiciel suspect, retirez-le de la liste !

CE QU'IL VOUS FAUT

> Zonealarm (gratuit)

www.zonealarm.com

DIFFICULTÉ

SELECTION LOGICIELS

BtProx > Verrouillage de poste

Très ingénieux, BtProx propose une solution originale pour éviter que des petits curieux ne fouillent dans votre PC en votre absence.

Il vous suffit d'un simple appareil Bluetooth (téléphone, iPod, etc.). Une fois configuré, le logiciel fermera votre session dès que votre appareil ne sera plus dans la portée du champ Bluetooth de votre ordinateur. Gadget donc indispensable...

http://btprox.sourceforge.net

ThreatFire > Protection résidente

ThreatFire propose de protéger votre système des processus dont l'activité est nocive pour la stabilité de votre système. Il agit, en fait, comme un antivirus équipé d'une protection résidente. Fonctionnant sans base de signatures, ce logiciel permet donc de se prémunir des attaques encore inconnues. La version gratuite ne propose pas de scan antivirus mais vous pouvez sans problème l'utiliser pour surveiller les activités autour de vos ports en plus de votre firewall. Un complément idéal !

www.threatfire.com

Revealer Keylogger Free > Keylogger

Un keylogger est un programme qui sert à enregistrer les frappes au clavier. Utilisé par les pirates pour voler des mots de passe et autres

informations délicates, il peut aussi être d'un grand intérêt pour vous ! En effet, vous garderez une trace des conversations et des recherches qui sont réalisées en votre absence sur votre PC. Il est de surcroît invisible pour vos «victimes».

www.fr.logixoft.com

Le B.A.-BA de la sécurité : LE MOT DE PASSE...

Garant de notre sécurité et de notre vie privée, les mots de passe ont envahi notre petit monde. Pour être efficace ces derniers doivent bien sûr être tenus secret mais ils ne doivent pas être oubliés non plus... Voici des outils et des conseils pour optimiser cet aspect.

L'arnaque type

Un Internaute a dernièrement été victime d'un pirate. Ce dernier a envoyé des courriels depuis le compte Gmail à tous ses contacts en leur indiquant qu'il était à l'étranger, qu'on lui a volé tous mes papiers et qu'il avait besoin de 1 000 € ! Parfois la supercherie peut durer des semaines...

Qui a accès à votre compte ?

Google fait des efforts pour améliorer son service et dernièrement une parade a été trouvé pour savoir si quelqu'un surveille votre compte. La dernière activité sur le compte apparaît en bas de votre page. Un lien **Détails** permet également d'accéder à un historique détaillé sur l'activité du compte : type d'accès (via POP, via le navigateur, via un mobile, etc.), adresse IP et date de la connexion.

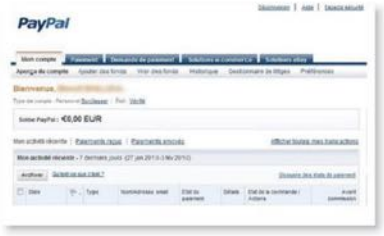
La robustesse

On peut juger la robustesse d'un mot de passe à partir de sa longueur (plus de 8 caractères), le type de caractères utilisés (majuscules, minuscules et caractères spéciaux) et sa durée de vie (un mot de passe doit être changé tous les six mois). Un site pour tester votre mot de passe : **http://cs76.free.fr/test-mot-passe.php**

Il suffit de faire une recherche sur Google pour constater le nombre incalculable de cas de vol de compte MSN, eBay, Paypal, Gmail ou autre. Lorsque vous vous faites pirater, vous n'avez plus moyen d'accéder à votre compte et aux informations qui y sont contenus. Pour reprendre le contrôle de ce dernier, il faut s'armer de courage et de patience puisque les cas sont nombreux et il est parfois difficile de prouver sa bonne foi. Surtout que les informations que les pirates peuvent récupérer (adresse, mots de passe, date de vacances, situation de famille, numéro de téléphone, etc.) facilitent l'accomplissement d'autres méfaits.

Le mot de passe : la clé du problème

En premier lieu, ne pensez pas «*je ne suis qu'un humble Internaute parmi tant d'autres, mes informations n'intéressent personne*». Toute information peut avoir de la valeur et c'est sans compter la simple volonté de nuire. Attention aussi aux utilisateurs de Paypal, d'eBay, de Google AdSense, de banque en ligne ou des webmasters qui mettent toute leur énergie dans leur site/blog et qui n'auront plus que leurs yeux pour pleurer en cas d'usurpation d'identité. Pour éviter la dépression nerveuse ou la banqueroute, n'utilisez jamais un même compte mail pour une utilisation professionnelle et personnelle. Ensuite, n'utilisez pas le même mot de passe pour plusieurs comptes mails ou plusieurs services. Ne prenez jamais un mot de passe qui veut dire

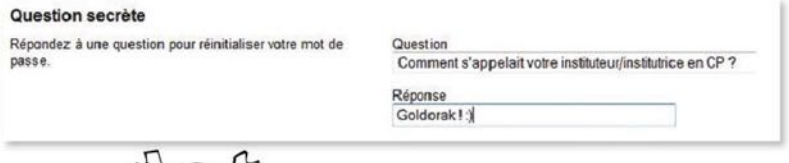


▲ **Un Gmail piraté va souvent de paire avec un Paypal dévalisé**

quelque chose (ou qui se trouve dans un dictionnaire) : alternez les capitales, les minuscules, les chiffres et les caractères spéciaux (voir le logiciel PassX page suivante).

La question d' «insécurité»

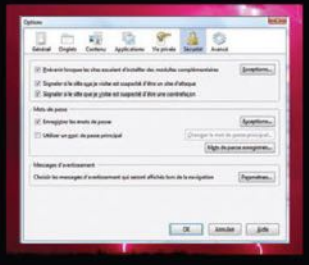
De même, n'utilisez pas de mots de passe permettant de deviner les autres : jesus75, jesus99 et jesus01 sont à bannir ! Ne cliquez jamais sur la petite case magique qui vous propose de mémoriser votre mot de passe si vous n'êtes pas sur votre machine ou si vous n'êtes pas le seul à y avoir accès. La fameuse question de sécurité pour retrouver un mot de passe n'est pas sûre. Le nom de jeune fille de votre mère ou la marque de votre première voiture ne sont pas des informations confidentielles (surtout si votre douce maman s'appelait Durand et que votre 205 junior tunée est sur votre Skyblog). Une technique consiste à répondre de la même manière à chaque question. Votre instituteur de CP ? Goldorak ! Le deuxième prénom de votre père ? Goldorak !



MOTS DE PASSE

Gmail hacké ?

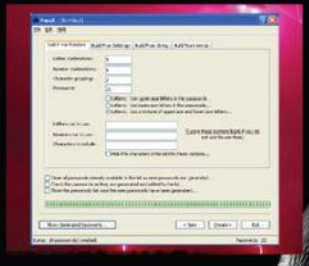
Si vous vous rendez compte d'un problème sur votre Gmail, il faut en premier lieu avertir Google. Allez à cette adresse : **http://mail.google.com/support** et cliquez sur **Impossible d'accéder à mon compte Gmail**. Remplissez les champs et il ne vous reste qu'à attendre et prier. Vérifiez ensuite que vous avez accès aux différents services auxquels vous êtes abonnés (Facebook, eBay, Paypal, etc.) Si vous ne pouvez y avoir accès, prévenez-les le plus vite possible. De même, prévenez les personnes qui étaient dans votre liste de contact. Il est d'ailleurs utile de faire une sauvegarde de cette liste avant de ne plus y avoir accès...



Firefox > Afficher vos mots de passe en clair

Si avec Firefox, vous avez enregistré vos identifiants et vos mots de passe pour accéder plus rapidement à vos sites et services favoris (tracker, forum, messagerie, etc.), il y a un moyen très simple de les retrouver. Dans Firefox, cliquez sur le menu **Outils, Options** puis choisissez l'onglet **Sécurité.** En cliquant sur le bouton **Mots de passe enregistrés**, vous verrez les identifiants correspondants aux sites. En cliquant sur **Afficher les mots de passe** puis en validant, les mots de passe sont affichés en clair.

www.mozilla-europe.org



Password Revealer > Gestion de mots de passe

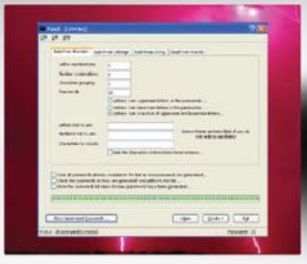
Password Revealer permet de révéler les mots de passe qui sont inscrits dans un champ spécial. Vous savez les étoiles ou les points qui masquent ce que vous avez tapé ? Il s'agit en fait de récupérer un de vos mots de passe pour le changer ou d'en retrouver un pour l'utiliser sur une autre machine. Il suffit de cliquer sur le bouton **Pister** pour commencer la recherche. Attention tout de même à ne pas laisser les mots de passe en clair si vous n'êtes pas le seul à accéder à votre ordinateur !

www.rekenwonder.com

Firefox > Mot de passe principal

Lorsque vous faites mémoriser vos mots de passe par Firefox, il est possible de définir un mot de passe principal qui débloquera tous les autres. Ce mot de passe vous sera demandé une fois par session, lorsque Firefox aura besoin d'accéder aux données qu'il a enregistrées. Dans Firefox, cliquez sur le menu **Outils** puis sur **Options**. Ouvrez alors l'onglet **Sécurité** et dans la zone de **Mots de passe**, cochez la case **Utiliser un mot de passe principal**. Tapez votre mot de passe et validez deux fois. À présent, lorsque vous souhaiterez utiliser un mot de passe enregistré ou en ajouter un nouveau, votre mot de passe principal vous sera demandé.

www.mozilla-europe.org



PassX > Générateur de mots de passe

PassX est un logiciel permettant de générer des mots de passes sécurisés. Il est possible de les générer complètement par hasard ou de les créer à partir d'une source (phrase, noms, titre d'une chanson ou de film, etc.). Idéal pour ceux qui n'auraient pas d'imagination ou peu de mémoire, toutes les configurations peuvent être sauvegardées et utilisées plus tard et les mots de passe générés peuvent être sauvegardés dans un fichier texte.

www.troupware.com

Jeux vidéo : UNE COPIE À L'IDENTIQUE!

Pour éviter de sortir un jeu de sa boîte et ainsi éviter de l'endommager, vous pouvez toujours le copier. La solution la mieux adaptée pour cela reste la création d'une image : une copie parfaite d'un CD/DVD au format numérique. Vous pourrez ensuite l'utiliser telle quelle avec Daemon Tools ou la graver si le cœur vous en dit...

Afin de ne pas risquer de rayer votre précieux CD ou DVD de jeu, il est possible de créer une image de celui-ci sur votre ordinateur. Pour ce faire, il suffit d'utiliser votre logiciel de gravure habituel. Selon la version, le procédé change quelque peu. C'est pour cela que nous utiliserons le logiciel gratuit CDBurner XP Pro. Qu'il s'agisse d'un jeu, d'un DVD Vidéo ou d'un logiciel, l'image sera la copie conforme de votre galette. Dans le cas qui nous intéresse (copie de jeu), nous utiliserons ensuite ce fichier image avec Daemon Tools pour pouvoir jouer comme s'il s'agissait du DVD d'origine…

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. Il ne s'agit bien évidemment pas d'une photo mais d'une copie conforme de ce que l'on trouve sur le disque d'origine, le tout en un seul fichier. 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 via Windows. Une fois gravée sur un CD/DVD, la boîte s'ouvre et on peut profiter du contenu. Daemon Tools «ouvre la boîte» sans avoir à graver quoi que ce soit...

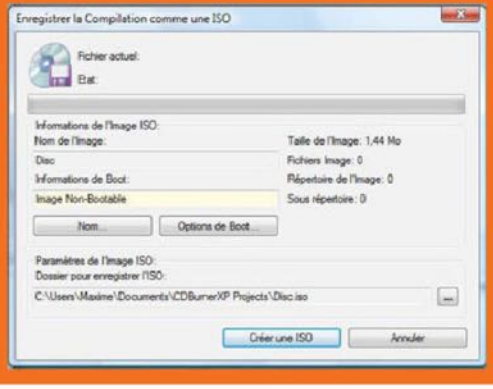
Convertir en ISO

Si jamais votre fichier image n'est pas un ISO, il est possible de le convertir via la commande Convertir en ISO accessible depuis la fenêtre de recherche de fichier. CDBurner XP Pro permet de transformer un fichier NRG (format de Nero Burning Rom) ou BIN en ISO.

PRATIQUE ▶ Créer et graver

1 Enregistrer un ISO

Pour créer une image de disque dans le but de sauvegarder un jeu, allez dans le menu **Fichier** de CDBurnerXP Pro puis choisissez **Enregistrer l'image comme un fichier ISO**.



Daemon Tools, l'ami des images

Nous avons vu qu'il n'est pas possible d'utiliser une image telle quelle avec Windows. Une image a en effet pour but d'être gravé un jour où l'autre pour restituer son contenu. Daemon Tools triche un peu en créant des lecteurs de DVD virtuels sur votre PC. Ils seront visibles dans votre poste de travail comme n'importe quel lecteur physique relié à votre carte mère. Le but de la manœuvre est de pouvoir lire les images de CD ou de DVD que vous téléchargez sur le Net ou que vous aurez créées avec votre logiciel de gravure. Le point fort de ce soft est qu'il est compatible avec la plupart des types d'images disques existants (voir notre encadré) et qu'il offre, en plus, plusieurs autres types d'options comme le lancement d'une image au démarrage ou un «montage» automatique. La version «Lite», gratuite, que nous vous proposons de découvrir, ne comporte pas d'interface graphique très poussée mais elle a le mérite de pouvoir faire à peu près ce que l'on veut avec ses images et comprend maintenant des menus en français…

Un logiciel sur la sellette

Daemon Tools va encore plus loin en proposant de lire les images des jeux protégés par un système anti-copie. Si vous n'arrivez pas à copier un jeu en le gravant, il suffit de créer une image standard et de la «monter» (la faire fonctionner) avec Daemon Tools.
En effet, ce dernier permet de faire sauter les 4 protections les plus utilisées dans l'industrie des jeux vidéos : SafeDisc, SecuROM, LaserLock et RMPS. Bien sûr le logiciel n'encourage pas le piratage (pourquoi ne pourriez-vous pas copier un jeu qui vous appartient ?) mais il est tout de même dans le collimateur des syndicats d'éditeur de jeux. Vous trouverez, sur le site, une base de données qui répertorie les jeux PC avec le type de protection utilisée, la version et parfois des commentaires. Outre cet aspect un peu spécifique du logiciel, Daemon Tools est de loin la solution la plus simple pour jongler avec des images sans avoir à les graver d'abord…

CE QU'IL VOUS FAUT

> CDBurner XP Pro (gratuit)
http://cdburnerxp.se
> Daemon Tools (gratuit)
www.daemon-tools.cc

DIFFICULTÉ

Sans Daemon Tools !

Si vous n'utilisez pas Daemon Tools et que vous voulez absolument graver un jeu protégé, il faudra connaître exactement le type d'algorithme utilisé pour pouvoir ensuite le contourner avec votre logiciel de gravure (CD-Mate par exemple permet de contourner certaines protections). Pour cela, nous utiliserons ClonyXXL. Vous trouverez ce petit logiciel ne nécessitant aucune installation ici : **www.gravure-news.com/html/download/24.php**. Il suffit de le

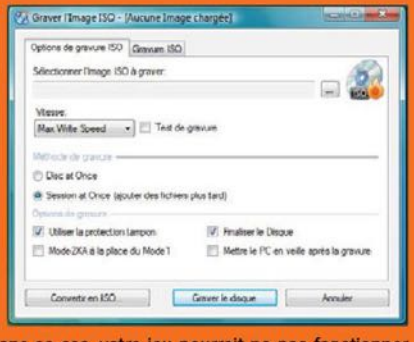
lancer et de cliquer sur Scan Disc en ayant bien sûr mis votre jeu dans votre lecteur. Au bout de quelques secondes, le logiciel vous informe de quelle protection est utilisée par votre jeu (ici SafeDisc v2.6). Lors de la gravure avec CD Mate, il suffira de spécifier la protection pour obtenir un clone de votre jeu...sans la protection.

une image

2 L'image

Dans la fenêtre qui s'ouvre, vous pourrez donner un nom à votre image et choisir si vous voulez en faire un disque bootable. Bien sûr dans le cas d'un jeu, cette option est inutile.Spécifiez ensuite un emplacement et cliquez sur **Créer une ISO**. Vous avez votre image ! Vous pouvez, également, utiliser un autre logiciel de gravure pour réaliser cette opération. il suffit généralement de trouver dans le menu l'option **Graver une image disque** ou **Graver une image ISO**.

3 Graver ?



Lorsque vous aurez décidé de graver votre image, choisissez **Créer un CD/DVD de données** puis allez dans **Fichier**. Dans ce menu, cliquez dans **Graver un disque à partir d'image ISO**. Parcourez ensuite le contenu de votre disque dur à la recherche de votre fichier et n'oubliez pas de valider en cliquant sur **Graver le disque**. Attention, dans ce cas, votre jeu pourrait ne pas fonctionner car CDBurner XP Pro ne contourne pas les protections de jeu. Dans l'hypothèse d'un jeu protégé, il faudra conserver l'image sur votre disque dur et l'utiliser avec Daemon Tools (voir plus loin).

Les images compatibles

Chaque logiciel de gravure dispose de son propre format de fichier d'image, ce qui rend parfois difficile de graver une image trouvée au hasard sur le Net. Vous n'allez tout même pas acheter 10 logiciels pour pouvoir graver votre précieux CD/DVD ! Sur les réseaux P2P, vous pourrez tomber sur ce type de fichiers... Ne les jetez pas, essayez de les lancer avec Daemon Tools !

- **ISO/CUE** Format d'image standard
- **CDI** DiscJuggler
- **CCD** CloneCD
- **NRG** Nero Burning Rom
- **ISZ** ISO compressé
- **PDI** Instant CD/DVD
- **MDS** Media Descriptor Sheet
- **BWT** BlindReag

... et bien d'autres

PRATIQUE

Monter une image dans un lecteur virtuel

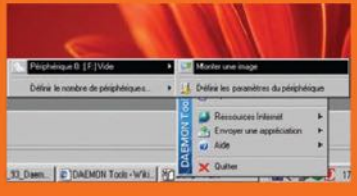
1 Montez votre image !

Une fois l'installation terminée, Vous trouverez alors, dans la barre des tâches, près de l'horloge, l'icône de Daemon Tools (un éclair rouge). Que vous ayez créé votre image avec un logiciel spécialisé ou que vous l'ayez trouvé sur le Net, il faudra «monter» cette dernière sur un lecteur virtuel. Par défaut, Daemon Tools crée un lecteur virtuel (le lecteur **F** dans

notre exemple). Nous allons commencer par augmenter ce nombre en faisant un clic droit dans l'icône puis en allant dans **CD/DVD-Rom Virtuel**. Allez ensuite dans **Définir le nombre de périphériques** et choisissez le nombre que vous voulez. Notez que la version Lite ne propose que 4 lecteurs maximum mais la version Pro Advance (payante) permet d'en créer jusqu'à 32 !

2 Parcourez...

Il est ensuite temps de monter notre image dans un lecteur virtuel. Toujours avec le clic droit, allez dans **CD/DVD-Rom Virtuel** et trouvez la ligne **Périphérique 0: [X] Vide** (où X représente la lettre de votre lecteur



virtuel). Cliquez ensuite sur **Monter une image**. Une boîte de dialogue s'ouvre vous demandant d'indiquer l'emplacement de votre fichier. Parcourez votre disque dur à la recherche de votre image et validez.

3 Jouez maintenant

Votre fichier est maintenant devenu un disque virtuel dans un lecteur qui n'existe

pas physiquement ! Vous le voyez apparaître dans le **Poste de travail**, à côté de vos «vrais» lecteurs. Pour lancer votre logiciel ou votre jeu, il suffit de double cliquer sur cette icône !

4 Quid des protections ?

Dans le cas où votre jeu ne fonctionnerait pas, il faudra émuler aussi la protection. Allez dans le menu avec un clic droit puis

déplacez la souris dans **Émulation**. Si vous connaissez précisément la protection du jeu (grâce à Clonny XXL ou au site officiel de Daemon Tools, dans la rubrique **Game Database**), nous vous conseillons d'activer cette dernière et seulement celle-ci. Dans le cas contraire, vous pouvez toujours essayer de cliquer sur **Activer toutes les options**. Attention, il existe des risques de conflits dans ce cas...

DVD Decrypter, rien ne lui résiste !

DVD Decrypter est un petit utilitaire gratuit vous offrant la possibilité de sauvegarder vos DVD sur votre ordinateur au format ISO. Longtemps au centre de la polémique, DVD Decrypter permet, en effet, de contourner certaines protections.

Borderline ! DVD Decrypter flirte avec la limite. Entre droit commun et illégalité, il vous permet tout de même de sauvegarder vos DVD. Le droit français autorise les acheteurs de DVD à copier leur bien au titre de la copie privée, permettant ainsi de sauvegarder un bien légalement acquis. Ce droit est justifié par la taxe sur la copie privée dont s'affranchit de manière invisible tout acheteur de disque dur, de CD vierge ou de téléphone nouvelle génération. Il est, cependant, interdit d'outrepasser les systèmes de protection des DVD, même sous couvert de la copie privée. Attention donc, le logiciel peut conduire à des actes de piraterie. Au-delà de cet aspect polémique, DVD Decrypter est un outil extrêmement puissant. Vous pourrez sauvegarder tous vos DVD au format image et ainsi les regraver ultérieurement. Vous pouvez évidemment sélectionner une partie seulement du DVD et ne conserver, par exemple, qu'une seule partie des sous-titres et jeter la publicité à la poubelle. Indispensable !

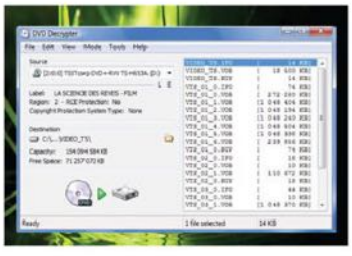
PRATIQUE ▸ Sauvegardez vos DVD !

1 Lancer

Le logiciel intègre une fonction d'intégration au menu contextuel. Ouvrez donc votre **Poste de travail** et faites un clic droit sur le lecteur DVD. Vous verrez alors apparaître l'option **Decrypt using DVD Decrypter**. Le logiciel se lance et affiche tous les fichiers présents sur le DVD.

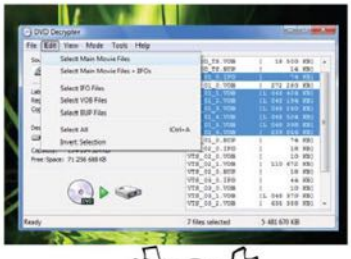
2 Décrypter

Référez-vous à notre encadré récapitulatif sur les extensions pour sélectionner les fichiers qui vous intéressent. Si vous possédez plusieurs lecteurs DVD, vous pouvez y accéder depuis le menu déroulant **Source**. Les autres informations concernent le nom du DVD (**Label**), la zone géographique concernée (**Region**), le niveau de protection anti-copie (**RCE protection** et **Copyright protection System Type**). Choisissez ensuite le dossier de destination à l'intérieur duquel vous souhaitez sauvegarder votre DVD.



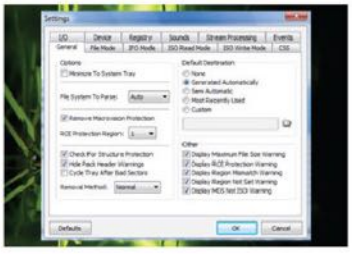
3 Le superflu

Sur tous les DVD, il existe de nombreux fichiers dont vous n'avez pas forcément l'utilité (publicité, films promotionnels, bonus, commentaires audio, sous-titres azerbaïdjanais, etc.). **DVD Decrypter** possède des filtres permettant de sélectionner automatiquement les fichiers intéressants. Allez dans le menu **Edit** puis cliquez sur **Select Main Movie Files**, ceci aura pour effet de mettre en surbrillance les fichiers audio concernant uniquement le film. Vous pouvez inverser la sélection (**Invert selection**) ou choisir d'autres types de fichiers.



4 Finalisation

Ceux qui souhaitent aller plus loin dans la création de la sauvegarde peuvent se rabattre sur l'onglet **Tools** et l'option **Settings.** Affichage des protections, sélection de la zone géographique, taille des fichiers de destination ou encore édition des informations sur les chapitres, vous aurez accès à de nombreuses options. Une fois votre choix opéré, il ne vous reste plus qu'à lancer le décryptage et la copie grâce à la fonction **Decrypt** dans le menu **File**.



CE QU'IL VOUS FAUT

> Dvddecrypter (gratuit)

www.dvddecrypter.org.uk

DIFFICULTÉ

Tout lire et tout copier... en HAUTE DÉFINITON !

Sur vos trackers Torrent, MegaUpload ou même la Mule, on voit de plus en plus de films avec la mention «HDRip». Il s'agit d'un rip (une copie) issu d'une source High Definition. Comment lire et copier une source HD ?

Vous le savez, les «sceners» (les passionnés qui mettent les films à disposition) aiment bien ajouter des abréviations à la fin des noms de fichiers pour que les P2Pistes soient sûrs de ce qu'ils téléchargent (voir notre encadré). Même si le phénémène n'est pas nouveau, on voit de plus en plus de nom de fichiers avec la mention «HDRip» ou «BDRip». Quelle qualité attendre de ces «releases», quels sont les logiciels à télécharger pour en profiter et comment faire votre propre HDRip ?

La source : le Blu-Ray

Ripper un DVD, c'est en extraire le contenu en vue de le réencoder dans un format moins gourmand en place (le DivX ou Xvid par exemple). Pour le HD Rip, c'est la même chose sauf que le format d'origine est le Blu-Ray (ou plus rarement le HD-DVD) et que le format de sortie est le MKV (Matroska) encodé grâce au codec h264. Comme les performances de compression du h264 sont supérieures au codec DivX et que la source est de meilleure qualité, le fichier encodé final possédera un meilleur rendu qu'un DVD. On trouve deux types de HD RiP correspondants aux deux principales résolutions de la Haute Definition : le 720p (1280x720) et le 1080p (1920x1080). Concernant le poids de ces fichiers, on tourne autour de 4.7Go pour un 720p et de 8.5Go pour le 1080p. Attention, le HDRip n'est pas de la vraie HD. Les fichiers seront lisibles sur un écran qui ne sera pas nécessairement HD Ready et sans les branchements HDMI ! De même, si vous voulez profiter de ces fichiers, sur une platine de salon, il faudra s'assurer que votre matériel est compatible avec le MKV encodé en h264. Parfois, on trouve aussi des BDRip (ou HD-R). Bizarrement, BD est l'abréviation pour Blu-Ray. Ces BDRip sont donc des fichiers image (généralement ISO) qui représentent un Blu-Ray Disc strictement identique au disque source. La taille de ces fichiers est donc énorme car un BD peut peser jusqu'à 40 Go ! Bien sûr, comme le format n'est pas modifié, un matériel compatible HD est nécessaire pour lire ces releases.

Problème de lecture ?

Si vous avez des difficultés à lire les HDRip, optez pour le logiciel VLC Media Player. Si le codec est un peu trop exotique, il faudra télécharger le pack de codecs K-Lite.

www.videolan.org/vlc
www.codecguide.com

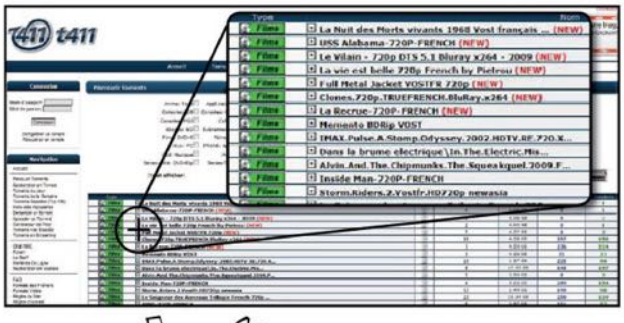
MPEG2 tanquille...

Une vidéo TS est un format spécial du MPEG2 (le format utilisé pour le DVD ou le BD). Pour la retravailler, il est préférable de la convertir en MPEG2 standard. Il est très facile de faire une telle manipulation avec le logiciel M4nG ou MediaCoder.

www.m4ng.com
www.mediacoderhq.com

Des blu-ray 128 Go ?

Sharp a dernièrement annoncer la mise en vente des premiers BD-R XL d'une capacité totale de 100 Go ! Il faudra bien sûr réinvestir dans du matériel compatible mais sachez que ces supports «triples couches» pourront aussi prendre en charge les disques quadruples couches de 128 Go !



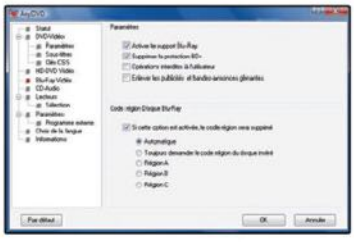
◀ Certains trackers ont même une section dédiée aux HD Rip et aux HD-R...

PRATIQUE

BLU-RAY : FAITES VOTRE RIP HD !

1 Le Rip

Pour commencer il faudra installer AnyDVD HD, le seul logiciel à pouvoir actuellement ripper un Blu-Ray. Vous avez 21 jours d'essai gratuit alors profitez... Allez dans les propriétés et assurez-vous que la case **Activer le support Blu-Ray** est cochée. Faites de même pour la case **Supprimer**



la protection BD+ et **Code région Disque Blu-Ray** (sélectionnez **Automatique**). Pour lancer le rip (l'extraction), faites un clic droit sur l'icône à tête de renard (à droite dans la barre des tâches) et choisissez **Ripper un DVD-Vidéo sur le disque dur...** Sélectionnez le répertoire de destination et cliquer enfin sur **Copier le DVD**.

2 Conversion en TS

Nous allons ensuite transformer le BD ainsi rippé en fichier reconnu par le logiciel M4ng. Lancez le logiciel et cliquez sur le bouton **Muxer/Demuxer** puis sur **Autres** et enfin **Mux (TSmuxer)** puis **Annuler** (pour virer la fenêtre qui viendra s'afficher). Ça y est, vous êtes dans TSmuxer. Cliquez ensuite sur **Add** et choisissez le fichier M2TS le plus gros de votre BD. Attention pour les utilisateurs de XP, il y a des chances que vous ne puissiez pas voir le contenu du BD dans l'explorateur Windows. Pour y remédier, trouvez et téléchargez au préalable les drivers UDF 2.5 sur Internet.

3 La vidéo et le son

Dans la fenêtre **Tracks**, vous devriez voir les différents fichiers vidéo, audio et sous-titres (PGS).
Sélectionner ce que vous souhaitez garder

comme audio et vidéo en cochant les cases correspondantes. Si l'audio est en AC3, pas de problème mais s'il s'agit de DTS-HD ou de TRUE-HD, il faudra cocher **Downconvert HD audio**. Plus loin, sélectionnez **TS muxing** ou **M2TS muxing** et choisissez le nom de votre fichier de sortie. Cliquer sur **Start muxing** et attendre la fin du processus.

4 Les sous-titres

Si vous voulez aussi ripper des sous-titres, il va aussi falloir passer par TSmuxer. Sélectionnez encore une fois le plus gros M2TS de votre BD puis trouvez la piste de sous-titre qui vous intéresse. Cochez **Demux**, choisissez un répertoire de destination puis **Start demuxing**. Vous obtiendrez un fichier SUP que nous modifierons avec SubRip pour le convertir en SRT.
Comme avec un DVD Rip, SubRip va apprendre de nouveaux caractères au fur et à mesure que vous l'utilisez. Cliquer sur **Open** pour choisir votre fichier SUP et cocher **Automatically continue with next subtitle** et cliquez sur **OCR**. Lorsqu'un caractère n'est

pas reconnu par le logiciel, il faudra le saisir au clavier. Normalement au bout d'un fichier de sous-titres, le logiciel ne vous demandera plus de l'aider. Pour les caractères spéciaux, cliquer sur **Character map**. À la fin, sélectionnez l'onglet **SRT**, vérifiez que votre travail est cohérent et cliquez sur **Save** pour enregistrer le fichier au format SRT. Nommez-le de la même manière que le fichier TS.

5 Encore M4ng !

Avec votre fichier TS et les sous-titres au format SRT, vous avez toutes les cartes en main pour les encoder au format désiré avec M4ng. Après avoir installé le logiciel (et éventuellement avoir fait une petite donation),

passez par le menu Ré-encodage (Expert). Ici, cliquez sur **Convertir TS ou DVR-MS en MPEG2** puis **Convertir une video TS...** Dans le menu **Fichier**, cliquer sur **Source** pour sélectionner le fichier TS à convertir. Une fois la conversion terminée, il faudra encoder ce MPEG2 en h264. M4ng le placera dans un conteneur MKV.

CE QU'IL VOUS FAUT

>Any DVD HD
www.slysoft.com

> M4ng
www.m4ng.fr

> SubRip
http://sourceforge.net/projects/subrip

DIFFICULTÉ

S'y retrouver dans les APPELLATIONS DE FICHIERS

Sur vos trackers Torrent, MegaUpload ou même la Mule, on voit de plus en plus de films avec la mention «HDRip». Il s'agit d'un rip (une copie) issu d'une source High Definition. Comment lire et copier une source HD ?

BDRIP > Rip d'un DVD Blu-Ray. Généralement de résolution de 720p ou 1080p, et encodé en X264.

BIVX > DivX incluant 2 bandes-son (version originale et version étrangère).

CAM > Une CAM est un enregistrement réalisé en filmant directement l'écran d'une salle de cinéma. Le son et l'image provenant d'une simple caméra vidéo, la qualité est, en général, assez faible. Le terme SCREENER est aussi utilisé en France mais de façon abusive (ci-contre).

DVB OU DVBRIP > Il s'agit d'un «Digital Video Broadcast», une copie issue d'une diffusion câble ou satellite. On trouvera aussi le terme SATRip.

DVD R > Il s'agit de la copie fidèle d'un DVD commercialisé (avec menu, langues, sous-titres éventuels, etc.). La vidéo est donc de qualité supérieure, non compressée. Mais le fichier est beaucoup plus lourd (plus de 4 Go).

DVDRIP > La source est un DVD du commerce mais l'auteur a extrait les seuls éléments qui pouvaient l'intéresser : la vidéo bien sûr mais peut-être aussi des sous-titres. Le fichier vidéo est le plus souvent compressé afin que le fichier final tienne sur environ 700 Mo ou 1,35 Go.

DVD-SCREENER, SCREENER ou DVDSCR > Ici, l'enregistrement est issu d'un DVD promotionnel, destiné aux journalistes, partenaires etc. Les producteurs y insèrent souvent des informations supplémentaires (bandeau informatif, numéros de téléphones, etc.).

HDTV > Ce terme signifie que la vidéo a été réalisée à partir d'un programme diffusé à la télévision en haute définition. On peut aussi trouver des annotations plus précises (720p, 1080p/i, etc.) pour définir le format HD en question.

LIMITED > Ce terme est en général attaché à un film qui n'a eu qu'une diffusion limitée dans les salles de cinéma (un court-métrage, par exemple).

PROPER > Il s'agit du terme le plus discutable de tous. Lorsqu'une team met à disposition un fichier dont une version est déjà existante, elle ajoute le terme PROPER pour signifier que son fichier est de meilleure qualité que le précédent.

R1, R2, R3, etc > C'est le code de la région de sortie d'une copie de DVD. Une information intéressante pour ceux qui recherchent des versions sorties dans un pays ou sur un continent en avant-première.

REPACK > Cette expression signifie que le fichier a été amélioré par rapport à la première version mise à disposition.

UNRATED > Peut être traduit par «Non censuré». En fait, il s'agit de films ou de versions de films n'ayant pas reçu d'avis et donc de limitations (coupe, âge, etc.) de la MPAA (Motion Picture Association of America).

TC > Assez rare, ce fichier a été édité par une source ayant eu accès à une copie digitale directement issue d'une bobine de film.

TELESYNC (ou TS) > C'est une version améliorée de la CAM. Ici, le son est enregistré depuis une source externe (par exemple, une prise destinée aux malentendants) et l'écran est filmé avec une caméra professionnelle.

VCD ou SVCD > Format Video CD compressé (Mpeg1 ou 2) compatible avec les lecteurs de salon, même si ces derniers ne prennent pas en charge les formats DivX.

VOST ou FRENCH SUB > Version originale sous-titrée : cela signifie simplement que la vidéo est disponible en version originale sous-titrée en Français.

VO ou VF > Version originale ou version française (doublage) tout simplement.

XVID, XVIDHD, H264, AAC, AC3, OGG > Tous ces petits vocables indiquent les formats et codecs vidéo ou audio avec lesquels ont été copiés les fichiers. Attention, vérifiez avant de télécharger que votre platine de salon les prend bien en charge si vous souhaitez les regarder sur votre télé, par exemple.

Un exemple d'intitulé de fichier torrent

Titre de la série

Le doublage est en Français

Codec utilisé pour la vidéo. Ici le Divx 6.

À la fin on trouve souvent le groupe qui a réalisé la copie : les «releasers»

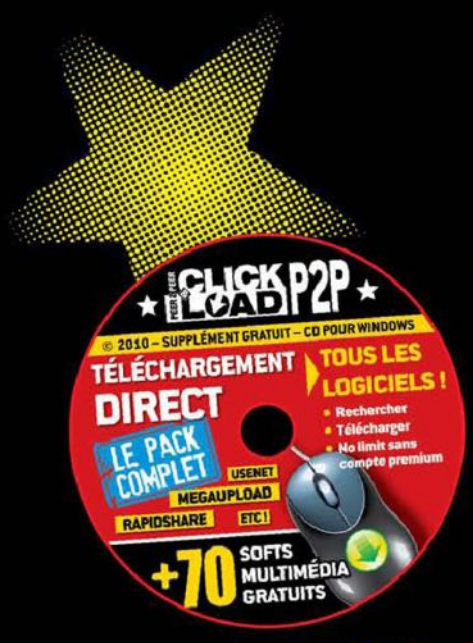
Prison Break.S02E06.FRENCH.DVDRiP.DivX6-PiMS.torrent

Numéro de l'épisode : ici c'est l'épisode 6 de la saison 2

La source. Ici un DVD du commerce

Ici nous avons affaire à un fichier torrent. Ce dernier doit être utilisé de concert avec un client adéquat, µTorrent, etc.

LIBRE ET ENGAGÉ

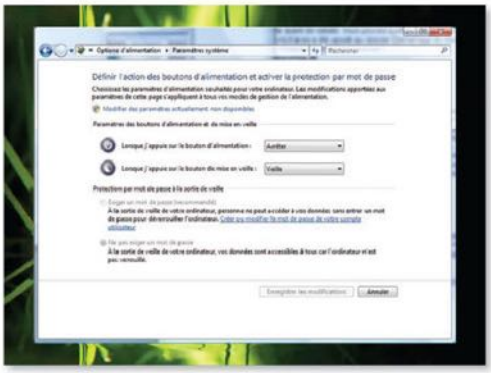


+ CD OFFERT !

VOTRE MAGAZINE
Nouvelle Génération

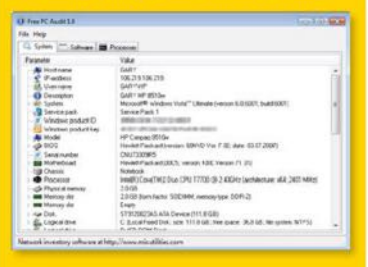
1 PROTÉGEZ VOTRE BUREAU
AVEC WINDOWS

Lorsque vous n'utilisez plus votre ordinateur, il se met en veille mais n'importe qui peut accéder à votre session. Pour protéger vos données, il est possible de demander à Windows de procéder à une saisie du mot de passe lors de la sortie de la mise en veille. Ouvrez le **Panneau de configuration** (depuis le **Poste de travail** pour XP et en faisant **Démarrer>Panneau de configuration** depuis Vista et 7. Dans la rubrique **Personnalisation**, allez vers **Écran de veille** puis **Modifier les paramètres d'alimentation**. Enfin, sur la gauche cliquez sur **Demander un mot de passe pour sortir de veille**. Dans cette fenêtre, cochez **Exiger un mot de passe**. S'il n'est pas possible de le faire cliquer sur **Modifier les paramètres actuellement indisponibles**. Enregistrez les modifications.



2 TESTEZ LES RÉSISTANCES DE VOTRE PC
AVEC PCAUDIT

Si vous vous posez des questions sur la sécurité de votre PC, pcAudit est un petit logiciel très pratique. Aussi bien pensé pour les particuliers que pour les administrateurs réseau ayant des données importantes à protéger, ce dernier va envoyer des données depuis



votre ordinateur vers un serveur d'Internet Security Alliance. S'il y parvient, il pourra alors déterminer les faiblesses de votre protection et vous propose une liste de conseils.

www.pcinternetpatrol.com

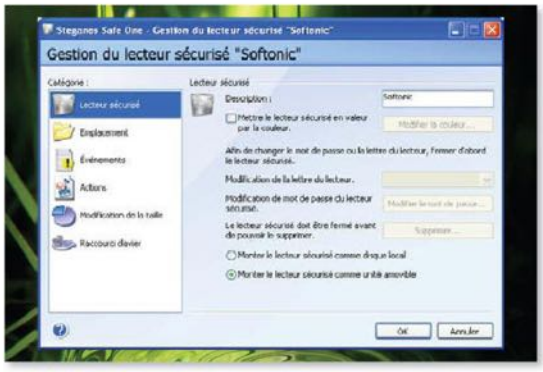
3 ANTI PHISHING
AVEC WEB OF TRUST

Le logiciel Web of Trust (WOT) permet de savoir si les sites sur lesquels vous surfez sont dignes de confiance. WOT se greffe sur votre navigateur en ajoutant une petite icône qui vous informe en un coup d'œil sur la confiance accordée à la page affichée : vendeur peu fiable, sécurisation du site à revoir, site non adapté aux enfants, etc. Les mêmes informations sont affichées lors d'une recherche sur Google, Yahoo ou Bing en face des occurrences. Grâce à sa base de données collaborative, vous éviterez le phishing, les malwares, etc.

www.mywot.com/fr

4 PARTITION SÉCURISÉE
AVEC SAFE ONE

Pour éviter aux regards indiscrets d'accéder à vos fichiers, il existe une solution plus radicale que d'avoir sa propre session. Il s'agit de créer un lecteur sécurisé sous



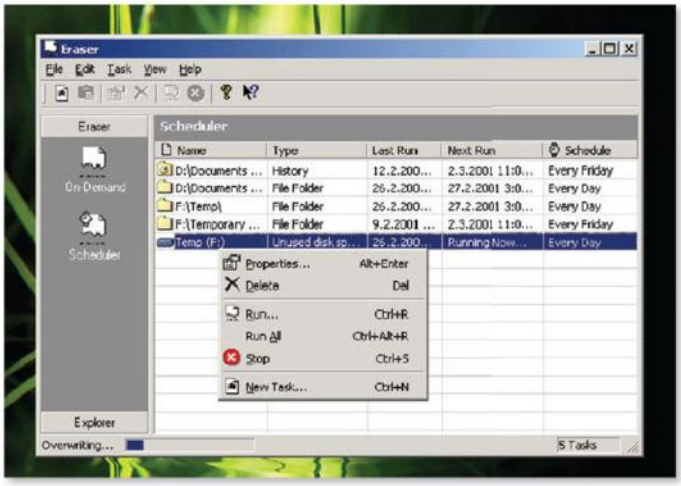
forme d'une nouvelle partition. Commencez par télécharger et installer le logiciel gratuit Safe One. Dans la fenêtre principale, cliquez à droite sur l'icône **Créer** pour installer un nouveau lecteur sécurisé. Cliquez deux fois sur le bouton **Suivant** et choisissez un nom et une lettre pour votre nouveau lecteur avant de valider. Vous devrez ensuite choisir la taille de votre lecteur. Notez qu'il n'est pas possible d'aller au-delà de 1 Go. Saisissez ensuite votre mot de passe (pensez à prendre un mot de passe suffisamment long et en alternant minuscules, majuscules, chiffres et caractères spéciaux). Une fois le processus de création terminée, vous devriez voir votre espace de stockage sécurisé dans le **Poste de Travail** (XP) ou dans **Démarrez>Ordinateur** (Vista et 7). Pour ouvrir votre espace sécurisé, ouvrez Safe One via le menu **Démarrer**, **Programmes**, **Steganos Safe One**. Cliquez sur le bouton **Ouvrir le lecteur sécurisé** et sur le bouton **Fermer le lecteur sécurisé** pour en sortir et rendre l'icône invisible. Comme un lecteur traditionnel, vous pouvez y créer des fichiers, les copier, les coller, etc.

www.steganos.com

5 EFFACER COMPLÈTEMENT UN FICHIER
AVEC ERASER

La suppression d'un fichier ou d'un dossier laisse des traces sur votre disque dur et ces données peuvent être récupérées grâce à des logiciels spécialisés... même après avoir vidé la corbeille. Si vous souhaitez effacer totalement certaines données sans aucune possibilité de récupération par une personne mal intentionnée, essayez Eraser. Ce logiciel va repasser plusieurs fois sur l'espace où est stocké votre fichier pour écraser toute trace de ce dernier. Une fois Eraser installé, faites un clic droit sur le fichier à supprimer. Sélectionnez **Erase** puis, dans **Options**, définissez le niveau de sécurité voulu. Par défaut, vous êtes au niveau maximum (qui implique 35 passes d'écriture sur votre fichier et donc un temps de traitement assez long). Une fois le processus terminé, Eraser vous présente son rapport !

http://eraser.heidl.le

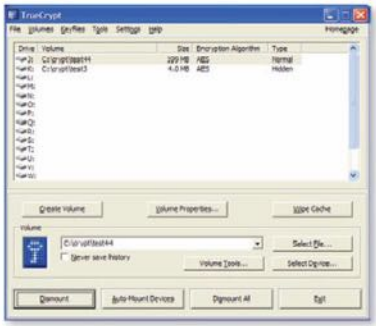


6 DES FORMULAIRES AUTOMATIQUE
AVEC AI ROBOFORM

AI RoboForm permet de remplir automatiquement les champs d'identification lorsque vous devez vous «logger». Il suffit de renseigner une bonne fois pour toutes vos informations personnelles : nom, téléphone, email, login, mot de passe, etc. Lorsque vous serez ensuite confronté à un formulaire, il suffira de cliquer sur AI RoboForm fill pour que le logiciel le remplisse automatiquement. AI RoboForm ne prend pas beaucoup de place et s'intègre parfaitement à votre navigateur Internet.

www.roboform.com

7 UN CRYPTAGE SUR MESURE
AVEC TRUECRYPT



Nous avons tous sur nos ordinateurs des données «sensibles» sous différentes formes : images, films, musiques mais aussi mots de passe, projets d'entreprise ou carnets d'adresses. TrueCrypt va vous permettre de crypter ces informations «à la volée». La sécurité est ici le maître mot puisque vous pourrez choisir parmi l'un des nombreux algorithmes de cryptage proposés (Blowfish, AES-256 bit, CAST5, Tripe DES, etc.) Après l'installation, il suffit de faire un clic droit dans un fichier ou un dossier puis de choisir l'action à accomplir dans le menu contextuel.

www.truecrypt.org

8 DIAGNOSTIC ANTIVIRUS EN LIGNE
AVEC HOUSE CALL

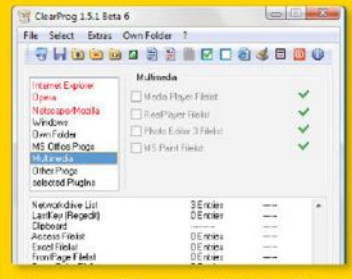
Voici le complément idéal d'un antivirus classique. Si votre cher Norton ne détecte rien ou s'il a un doute, pourquoi ne pas tenter

l'expérience en ligne ? Sur House Call, il est possible de scanner des disques durs ou ses périphériques de stockage sans rien installer. Il offre aussi un diagnostic gratuit de vos ports.

http://housecall.trendmicro.com/fr

9 FAITES LE MÉNAGE
AVEC CLEARPROG

Au lieu d'effacer les traces de vos surfs sur votre disque dur chaque jour "à la main", pourquoi ne pas automatiser cette tâche ? Téléchargez le logiciel gratuit ClearProg et après son lancement, vous verrez une liste des éléments que vous pouvez supprimer. Parcourez les différentes rubriques et décochez la case devant les éléments que vous souhaitez conserver. Cliquez ensuite sur le menu **Options** puis sur **Installer un**

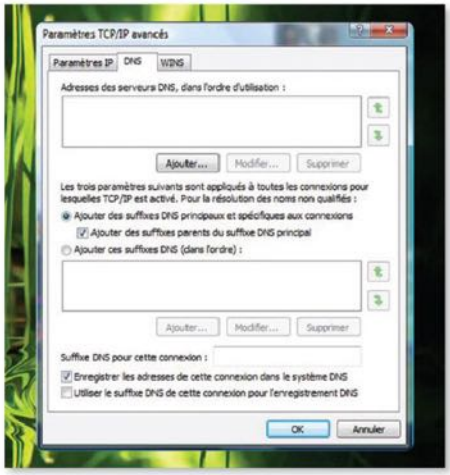


auto-raccourci. Dans cette fenêtre, cliquez sur menu **Démarrer** avant de valider. Vous pouvez quitter le logiciel : un nouveau raccourci lançant le nettoyage de vos traces a été ajouté au dossier **Démarrage** du menu . À chaque démarrage de Windows, le ménage sera fait !

www.clearprog.de

10 DÉBRIDER LE STREAM DE YOUTUBE
AVEC LA LIVEBOX ORANGE

Il s'agit d'un problème bien connu de certains abonnés d'Orange : une lenteur affligeante lors d'un visionnage de vidéo en stream sur YouTube ou d'autres sites de stream américains. Il s'agit apparemment d'un acte délibéré du FAI pour éviter de gaspiller de la bande passante. Si vous rencontrez ce problème, nous avons la solution ! Il suffit de changer vos DNS et opter pour ceux de Google. Allez dans le **Panneau de configuration**, puis dans le **Centre réseau** et enfin **Gérer les connexions réseau**. Sélectionnez la connexion pour laquelle vous souhaitez configurer les nouveaux DNS et faites un clic droit puis cliquez sur **Propriétés**. Ici, vous pouvez être invité à entrer un mot de passe administrateur ou une confirmation. Cliquez sur **Protocole Internet version 4 (TCP/IPv4)** puis sur **Propriétés**. Cliquez enfin sur **Avancé** et sélectionnez l'onglet DNS. Remplacez ces adresses avec les adresses IP des serveurs DNS de Google: 8.8.8.8 et 8.8.4.4. Redémarrez votre connexion ! Attention, avant de changer de DNS, il faudra bien noter les anciens chiffres au cas où vous voudriez revenir en arrière...



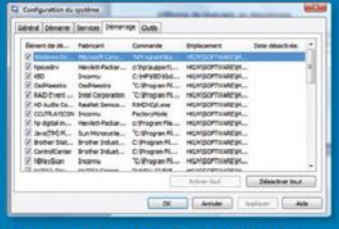
11 GÉNÉREZ VOS CLÉ WIFI
AVEC WIFI KEY GENERATOR

Comme son nom l'indique, WIFI Key Generator est un générateur de clés WEP/WPA/PSK. Si vous manquez d'imagination pour inventer une clé pour votre réseau WiFi, c'est la solution ! Le logiciel permet surtout de générer une clé de cryptage avec un degré de complexité suffisamment satisfaisant.
Si vous avez peur qu'un malotru vous vole votre précieuse bande passante, n'hésitez plus ! WiFi Key Generator permet de générer des clés jusqu'à 256 bits. Il est également possible de rédiger une "passphrase" de 63 caractères pour qu'il puisse générer une clé correspondante. N'oubliez pas de l'enregistrer consciencieusement dans un fichier texte !

http://atlex.nl/index/wifigen

12 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.

13 UNE CLÉ USB QUI OUVRE VOTRE SESSION

AVEC PREDATOR

Si vous n'aimez pas trop qu'on vienne sur votre PC sans être invité, il existe plusieurs solutions comme le verrouillage de session (raccourci clavier touche Windows + L). Le problème, c'est qu'on vous demandera à chaque fois de taper votre mot de passe. Predator sécurisera l'accès à votre ordinateur en transformant une de vos clés USB en véritable cadenas numérique. Vous n'aurez qu'à la retirer pour verrouiller votre session et il vous suffira de la réinsérer pour en débloquer l'accès sans avoir à saisir de mots de passe. Il y installera une clé secrète composée de 112 caractères, lettres majuscules et minuscules, chiffres, caractères spéciaux ainsi que le nom de votre machine et la date. Ce fichier au format CTL sera régulièrement mis à jour afin d'éviter qu'une copie de votre clé serve à entrer. Vous pouvez bien sûr utiliser

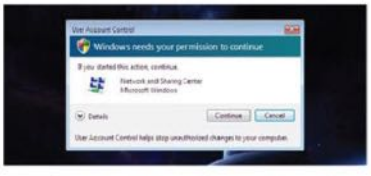
la clé USB comme unité de stockage puisque le logiciel ne prend que 9 Mo !

www.montpellier-informatique.com

14 DÉSACTIVER LE PÉNIBLE UAC

AVEC WINDOWS VISTA

Windows Vista intègre une nouvelle fonctionnalité nommée UAC (pour User Account Control). Son rôle est de contrôler l'administration de l'ordinateur en demandant une confirmation pour chaque exécution d'une tâche nécessitant un privilège élevé. Si cette fonctionnalité apporte une meilleure sécurité selon Microsoft, elle peut rapidement devenir très pénible. Pour supprimer ce fil à la patte, allez dans **Démarrer**, puis **Panneau de configuration**. Choisissez l'affichage classique sur la gauche et double-cliquez sur **Comptes d'utilisateurs**. Cliquez ensuite sur **Activer ou désactiver le**



contrôle des comptes d'utilisateurs. L'UAC vous demandera une confirmation (la dernière !), cliquez sur le bouton **Continuer**. Dans la nouvelle fenêtre venant de s'ouvrir, décocher la case **Utiliser le contrôle des comptes d'utilisateurs pour vous aider à protéger votre ordinateur** et cliquez sur **OK**. Redémarrer enfin l'ordinateur !

15 SAUVEGARDER LE REGISTRE

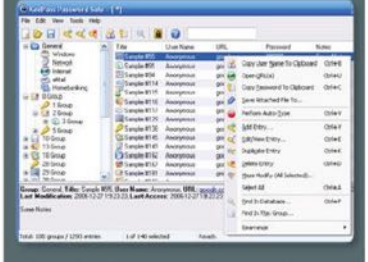
AVEC WINDOWS

Lors d'une contamination par un virus, la base de registre (qui garde en mémoire certains réglages) est une zone très sensible. Même avec un puissant antivirus, cette base de registre a de grandes chances de ressembler à du gruyère en cas de d'attaque. Pour ne pas avoir de surprise même lors d'une manipulation importante sur votre PC, il est conseillé de faire une sauvegarde de cette dernière. En premier lieu, il faut accéder à cette base. Dans XP, déroulez le menu **Démarrer**, cliquez sur **Exécuter**, tapez **regedit** puis cliquez sur **OK**. Pour Vista ou 7, déroulez le menu **Démarrer**, positionner le curseur dans la barre de recherche puis taper **regedit**. Ouvrez le menu **Fichier**, puis cliquer sur **Exporter**. Dans cette nouvelle fenêtre, choisissez de sauvegarder votre base de registre sur votre bureau ou dans une clé USB. Choisissez un nom du type **base_de_registre_avant-installation-photoshop_12-04-2010**. Avant d'enregistrer, vérifier bien que la case **Tout** est cochée dans **Étendue de l'exportation**. Pour restaurer le registre, double-cliquez sur le fichier que vous avez sauvé et la base de registre retrouvera son état d'origine. En cas d'échec, ouvrez à nouveau le registre et utilisez l'option **Importer** dans **Fichier**...

16 UN MOTE DE PASSE GÉNÉRAL

AVEC KEEPASS PASSWORD SAFE

Keepass est une sorte de grand coffre-fort pour tous vos mots de passe. Il permet de stocker ces derniers dans un seul et même fichier. Utilisant les algorithmes AES et Twofish, Keepass protège toute cette base de données par un seul et unique mot de passe. Il est aussi envisageable de requérir l'utilisation d'un disque amovible (comme une clé USB). L'interface permet



d'associer chaque mot de passe à une page Web, un commentaire, une date d'expiration. Il est aussi possible d'y attacher un fichier. Une fonction d'importation/exportation en mot texte ou XML permet de transférer la base de donnée depuis et vers d'autres logiciels.

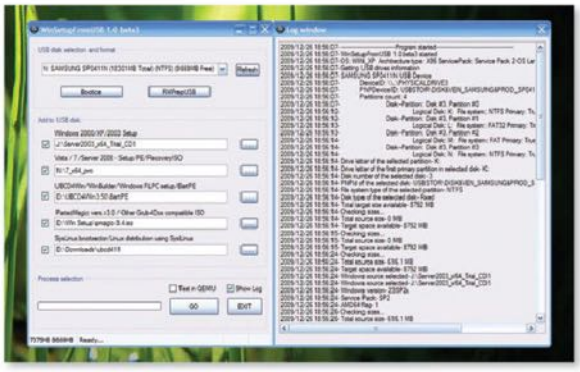
http://keepass.info

17 UNE COPIE AUTHENTIQUE
AVEC WINDOWS 7

Il arrive parfois que Windows 7 affiche un message mettant en doute l'originalité du système. Il s'agit bien sûr d'une erreur car comme tout bon citoyen, vous avez payé votre «redevance Microsoft». Pour éviter cette fenêtre, il va falloir réinstaller les fichiers de la licence. Tapez **cmd** dans le champ de recherche du menu **Démarrer** puis faites un clic droit sur **cmd.exe** pour sélectionner **Exécuter en tant qu'administrateur**. Saisissez alors **simgr /rilc** et confirmez par **Entrée**.

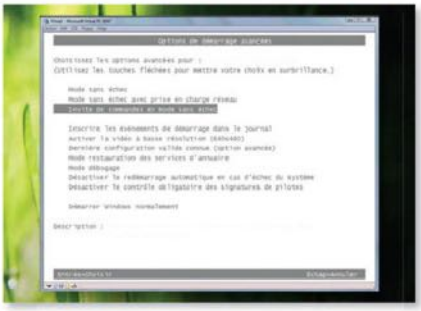
19 INSTALLER WINDOWS XP SUR UNE CLÉ USB
AVEC WINSETUPFROMUSB

Personne n'est à l'abri d'un gros problème sous Windows. Que vous soyez loin de vos précieux DVD d'installation lors d'un voyage ou que vous ayez à dépanner votre cousin Kévin (quel boulet celui-là !) il est bien pratique d'avoir un OS prêt à être installer sur un simple clé USB ! Un petit utilitaire très pratique permet en effet d'installer ou réinstaller Windows XP depuis un support amovible ! Très pratique aussi pour ceux qui n'ont pas de lecteur DVD (les fameux «Netbook» par exemple). Pour cela, il vous faut votre DVD d'installation de Windows XP, une clé USB d'au moins 1 Go et le logiciel WinSetupFromUSB. Installez et lancez le logiciel puis choisissez l'emplacement du lecteur DVD en cliquant sur **Browse** puis insérez votre clé USB avant de cliquez sur **Refresh**. Sélectionnez **Fixed** puis **Go** pour lancez la copie de Windows XP sur votre clé USB. Attention, il faudra aussi s'assurer que le PC sur laquelle vous voulez installer Windows XP accepte de booter depuis une clé USB (il suffit de faire un tour dans le BIOS en faisant **Suppr** ou **F1** au démarrage).



http://usbwin.c.la

18 DÉMARRER EN MODE SANS ÉCHEC
AVEC WINDOWS

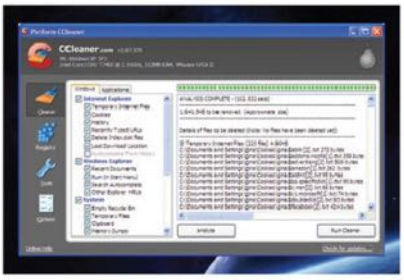


Il arrive souvent que Windows ou qu'un logiciel vous demande de redémarrer en mode sans échec pour résoudre un problème. Il s'agit d'un mode spécial qui ne charge aucun pilote au démarrage pour lancer Windows dans les meilleurs dispositions. C'est aussi le dernier recours pour faire démarrer son système d'exploitation. Redémarrez l'ordinateur, puis lorsque celui-ci va commencer à afficher la séquence du BIOS, commencez alors à appuyer sur la touche **F8** de votre clavier (parfois, il s'agit de **F5**). Windows devrait alors afficher un menu d'options. Utilisez votre clavier pour sélectionner **Mode sans échec** dans le menu et valider avec **Entrée**. Si l'affichage est bizarre c'est normal : votre carte graphique dernier cri ne fonctionnera pas dans ce mode. De même Internet ainsi que vos périphériques USB seront inopérants.

20 SUSPENDRE UN REDÉMARRAGE
AVEC WINDOWS

Il arrive que vous regrettiez d'avoir lancé l'arrêt de Windows ou que ce dernier croit bon de rédemarrer sans demander votre avis. Si vous voulez continuer ce que vous étiez en train de faire et suspendre ce redémarrage, cliquez sur le bouton **Démarrer** et saisissez rapidement la commande **shutdown /a**. Validez ensuite en pressant simultanément sur les touches **Ctrl**, **Maj** et **Entrée** afin d'exécuter la commande avec les droits d'administration. Toutes les demandes d'arrêt de Windows sont alors interrompues...

21 OPTIMISER VOTRE WINDOWS
AVEC CCLEANER



CCleaner est un petit logiciel qui fait office de couteau suisse pour votre PC. Il permet de faire le ménage (historique, cookie, etc.), de désinstaller proprement des logiciels mais aussi de faire du propre dans la base de registre. En effet à force d'installation et de réinstallation, votre pauvre base de registre ressemble de plus en plus à un morceau de gruyère. Pour colmater les brèches et gagner en efficacité, lancez l'application, cliquez sur **Registre** en haut à gauche puis sur **Chercher les erreurs**. Laissez le logiciels faire son œuvre puis choisissez **Corriger les erreurs sélectionnées** pour réparer votre base de registre. Lorsque Ccleaner vous propose de sauvegarder le registre, accepter sous peine de le regretter amèrement en cas de problème avec la phase de réparation...

22 ARCHIVE AUTO-EXTRACTIBLE
AVEC 7ZIP

Si vous avez un gros fichier à envoyer mais que vous n'êtes pas sûr que le destinataire ai un logiciel de décompression d'archive, il existe un solution toute simple : créer une archive auto-extractible. Plus besoin de logiciel pour vos destinataires et pas besoin non plus d'expliquer comment fonctionne Winzip ou Winrar !
7-Zip est un compresseur/décompresseur de fichiers très performant et surtout gratuit. Il permet d'ouvrir un grand nombre d'archives et compresse en ZIP, BZIP2, GZIP, TAR mais surtout dans son format 7Z qui permet d'obtenir le meilleur résultat. Installez ce logiciel et faites un clic droit dans le fichier à compresser. Choisissez **7zip** dans le menu puis **Ajouter à l'archive**. Dans le choix de l'archive, sélectionnez **7z** puis cochez la case **Créer une archive SFX** avant de valider. Votre destinataire n'aura qu'à double-cliquer sur ce fichier pour qu'il se décompacte automatiquement sans installation préalable...

23 ACTIVER LA RECONNAISSANCE VOCALE
AVEC WINDOWS VISTA

Vous ne le savez peut-être pas mais Vista propose un module de reconnaissance vocale. Si vous avez un long texte à taper ou si vous souhaitez simplement tester cette option, il faudra vous équiper d'un micro. Dérouler le menu principal puis cliquer sur **Tous les programmes>Accessoires>Options d'ergonomie** puis **Reconnaissance vocale de Windows**. Avant de pouvoir en profiter, le module débute par le choix et le calibrage du micro. Si vous le désirez, vous pouvez cocher la case **Lancer la reconnaissance vocale au démarrage** (ou créer un raccourci sur le Bureau pour y avoir accès plus facilement). La procédure débouche sur un tutoriel pour apprivoiser ce module, qui livre les commandes clés : **Commencer l'écoute** (pour que l'ordinateur obéisse à votre voix et à votre dictée), **Fin de l'écoute** et **Masquer l'écoute** (pour réduire la console de reconnaissance vocale dans la barre des tâches). Vous pourrez utiliser cette fonction pour lancer des programmes à la voix ou pour saisir un texte sans avoir à utiliser le clavier. Pour un meilleur résultat, il est conseillé d'enrichir le vocabulaire compris par la reconnaissance vocale.

24 UNE FAUSSE ALERTE
AVEC TOUS LES ANTIVIRUS

Rien de plus efficace pour tester votre antivirus que de le voir réagir à un problème dans de vraies conditions. Pas question d'essayer de chopper un virus pourtant ! Nous allons donc créer un faux virus : Eicar. Ce dernier est complètement innoffensif et a même été créer dans ce but ! Ouvrez votre Bloc-note **Démarrer>Exécuter**

puis tapez **notepad** ou directement **notepad** dans le champ de recherche de votre Vista ou 7) puis copiez la chaîne suivante composée de 68 caractères (sur une seule ligne) :

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Sauvegardez maintenant ce fichier texte sans oublier de changer son extention en .COM, .BAT ou .EXE. Si votre anti-virus est correctement installé et activé, il devrait instantanément vous alerter de la présence du virus Eicar. Vous pouvez également pousser plus en avant vos tests en compressant le fichier ou en le plaçant sur un clé USB,etc.

X-MATERIELS

> Un gadget à l'écoute...

Le CVKA-G108 est un émetteur audio utilisant la technologie GSM pour surveiller un lieu à la demande. Il suffit en fait de placer une carte SIM à l'intérieur et de téléphoner au numéro de cette même carte pour écouter tout ce qui se passe dans la pièce où vous avez mis l'appareil. Plus fort encore : comme vous ne savez pas toujours quand il se passera quelque chose, il est même possible de se faire prévenir par SMS lorsque l'appareil détectera du bruit ou des voix aux alentours. D'un simple coup de fil, vous savez donc qui se trouve dans votre maison, ce que font vos enfants ou si votre femme est bien allée faire des courses à Carrefour... Attention, même si ces appareils sont légalement en vente sur Internet, espionner des tiers à leur insu est puni par la loi...

Prix : **27 €** www.chinavasion.com

> Le stylo 007

Si vous avez besoin d'une caméra espion à hauteur de corps, rien n'est plus simple ou discret que de placer ce stylo caméra dans une poche de chemise pour une vue imprenable sur ce qui est en face de vous. Grâce à ses fonctionnalités d'enregistrement audio et vidéo couleur et ses 2 Go de mémoire interne, ce qui permet de stocker près de 50 minutes de film, vous pouvez commencer à filmer sans vous soucier du reste. Accrochez-le sur votre poche et promenez-vous à l'endroit que vous souhaitez filmer, ou laissez-le à un endroit donné pour enregistrer une conversation. Pour les enregistrements dans un environnement de bureau, placez-le dans un porte-crayon ou tout au moins de façon naturelle, comme un stylo oublié sur le bureau. Dévissez le stylo espion pour révéler un connecteur USB soigneusement masqué, de façon à pouvoir brancher le stylo sur un ordinateur et procéder à un transfert de fichier immédiat. Si vous êtes dans une situation délicate ou si le facteur temps est crucial, vous pouvez effectuer un enregistrement secret, puis le joindre à un message et le charger sur Internet en quelques minutes. Idéal pour les détectives privés ou les journalistes d'investigation, le stylo caméra est un outil essentiel pour toutes les tâches de surveillance.

Prix : **50 €** www.coindugeek.com

> A la Splinter Cell !

Si vous êtes fan des gadgets du GIGN ou si Sam Fisher (ha Splinter Cell !) est votre héro, ce gadget un peu coûteux a des chances de vous intéresser... Il s'agit d'une caméra équipée d'un câble flexible et étanche d'un mètre (diamètre de 7,5mm). Elle rend simple l'accès à des zones difficiles : toit, mur, dessous de porte, trou dans une cloison, abri de marmotte, etc. Compacte et facile à utiliser, l'extrémité de son câble à aussi deux LEDs (petites lampes) pour éclairer les zones sombres. Le corps de l'appareil est équipé d'un écran de 2,5 pouces (6,4 cm) permettant de visualiser clairement la zone inspectée avec une résolution de 704x576 pixels. Attention, cette caméra ne doit pas être confondue avec des versions de qualité inférieure. Cette caméra est très précise (704*576 pixels en PAL) et son tube d'inspection est étanche.

Prix : **190 €** www.top-espion.com

> Un détecteur de micro !

Un peu comme dans les film d'espionnage, cette espèce de télécommande compacte (93x48x17mm) détectera toutes émissions de fréquence entre 100 MHz et 6.5 GHz. Ce qui veut dire qu'une fois mis en marche le détecteur vous signalera si un émetteur se trouve dans la pièce où vous vous trouvez. Attention, les réseaux WiFi en font aussi partie mais la cadence d'allumage de la LED (ou des vibrations) sera un indice de la localisation du micro. Ce détecteur détectera sur ses plages de fréquences des micros espions sans fils, des caméras espions sans fils, des émetteurs infinis en utilisation, etc. En ce qui concerne les caméras filaires (qui n'ont pas d'émission de fréquence et ne peut donc pas être détectée par un détecteur ordinaire), cet appareil a une série de lentilles infrarouges qui illumineront les lentilles des caméras cachées. En regardant à travers son objectif vous pourrez ainsi repérer certaines de ces caméras...

Prix : **85 €** www.top-espion.com

NOTRE TEST EXCLUSIF

·····> L'émetteur audio GSM CVKA-G108

Pour la modique somme de 32 €, port compris (attention si cet objet vous intéresse, il est préférable de passer par le site **www.chinavision.com** car les sites européens doublent les prix pour ce genre d'appareil) ce CVKA-G108 est livré avec un câble USB, un chargeur et une notice en anglais très mal traduite (**Fig 1**)

L'appareil en lui-même est assez petit (52 x 40 x 15 mm) pour être dissimulé dans une pièce, dans une voiture ou un sac à dos mais malheureusement un peu trop gros pour le mettre dans un petit sac ou dans la poche de votre "victime". Comme il est quadribande, vous pouvez mettre une carte SIM française sans problème mais attention, lors de notre test avec une carte SFR, l'appareil a refusé de fonctionner. Il faudra donc comme nous passer par une SIM prépayée ou émanant d'un opérateur indépendant comme Simyo par exemple. Après insertion de votre carte SIM à l'intérieur de l'appareil (attention le clapet est un peu récalcitrant), il suffit d'envoyer un message texte au numéro de cette carte contenant les lettres d'activation comme indiqué dans le manuel d'utilisation (dans notre cas, "GDM" suivi de votre numéro de téléphone cellulaire, **Fig2**).

Votre "bug" est actif et prêt à l'action ! Vous aurez remarqué qu'en dessous du slot pour la SIM il y a un interrupteur comptant 2 positions : A et B (**Fig 3**).

La première option correspond à l'espionnage "à la demande" : un simple coup de fil et vous êtes à l'écoute quand vous le voulez. En position B, l'appareil vous enverra un SMS lorsqu'il calculera une présence sonore. Si personne n'est censé se trouver chez vous et que vous recevez un SMS, à vous de téléphoner pour savoir si vos enfants font la fête ou si un cambrioleur essaie de voler votre collection de Picasso... Malheureusement, cette fonction n'a jamais marché avec notre appareil. Problème de fabrication ? Le service après-vente qui devait entrer en contact avec nous par e-mail n'a jamais daigné le faire. Lors de nos tests nous avions placé l'émetteur près de haut parleur pour voir si le fait d'émettre pouvait générer des interférences mais rien à signaler ! Le son n'est pas vraiment de bonne facture mais les conversations non chuchotées sont parfaitement audibles jusqu'à 5m. Il ne vous reste qu'à placer la bête dans un endroit approprié (**Fig 4**).

En ce qui concerne l'autonomie, le constructeur indique 3 à 5 jours en veille et 3 heures en écoute mais il est assez difficile de se faire une idée précise puisqu'au moment où vous vous mettez sur écoute, l'appareil est peut-être déjà en veille depuis quelques heures. Comptez 8 heures pour une recharge complète. Heureusement, à la maison, vous avez la possibilité de laisser le CVKA-G108 branché sur une prise secteur... Attention, le chargeur, conformément à notre demande est de type «européen» mais les fiches ne sont malheureusement pas assez longues pour rentrer dans une prise standard de sécurité. Il faudra que vous rechargiez l'appareil sur l'ordinateur via son port USB, à moins d'avoir de vieilles prises à la maison...

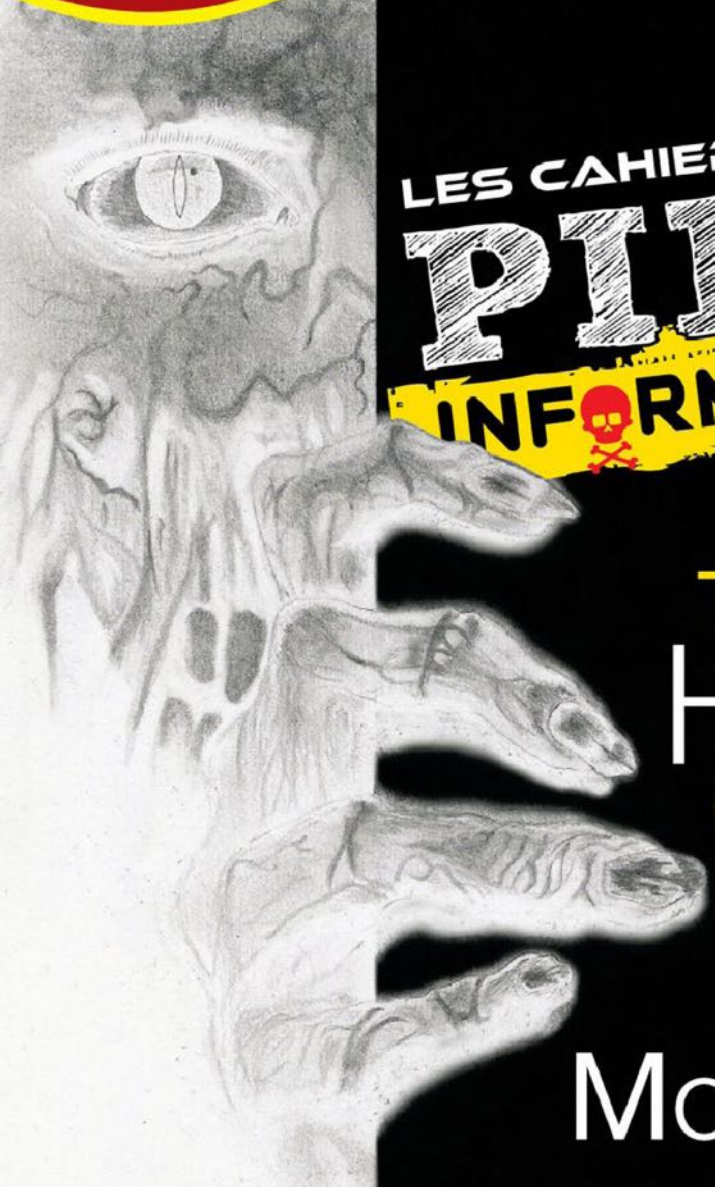
CD OFFERT

LE PACKAGE DU PIRATE

Tous les logiciels INDISPENSABLES

LES GUIDES PRATIQUES

100% MICRO-FICHES, TRUCS & ASTUCES



LES CAHIERS DU HACKER

PIRATE INFORMATIQUE

PIRATAGE DE COMPTES

TÉLÉCHARGEMENTS

HACKING

CRYPTAGE WAREZ

ANONYMAT

SURVEILLANCE

MOTS DE PASSE

RÉSEAUX DÉBRIDAGE

CONTRÔLE À DISTANCE

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

L 12730 - 7 - F: 4,90 € - RD