

TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

100% DE PUBLICITE JUSTE DES ARTICLES 2,00 €

www.hackernewmag.it
HACKER
news
Magazine

UN SERVEUR
eDonkey
POUR TOUS

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

SCANNER
UN RÉSEAU
en tout simplicité

CRACKER
UN MOT DE PASSE
TOUT UN ART!

CACHER
tous ses fichiers
et **EFFACER** ses
traces en ligne

D'échelon aux **soywares**

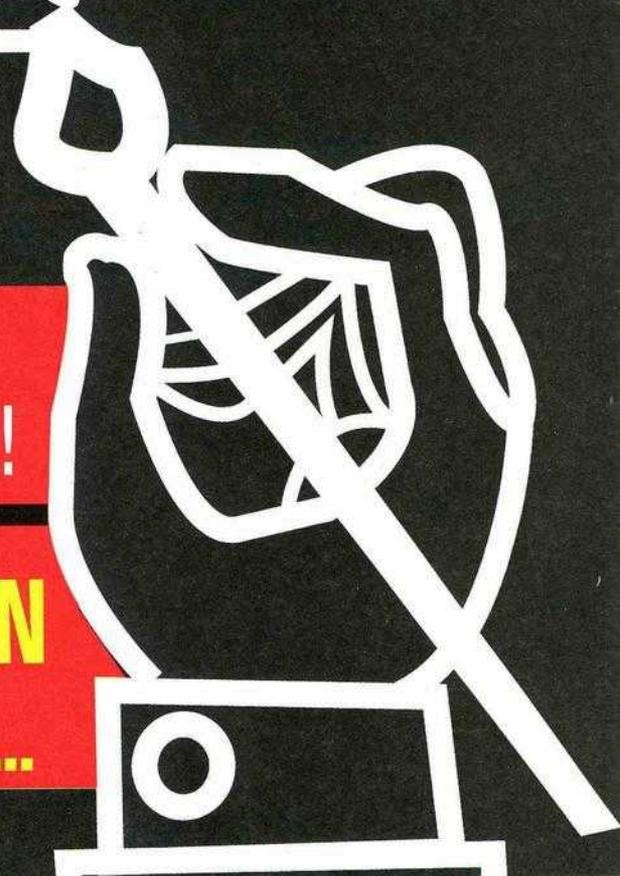
**BIG BROTHER IS
WATCHING YOU!**



je participe
tu participes
il participe
nous participons
vous participez
ils profitent

Les majors ne défendent pas les
intérêts des artistes, mais les leurs !

**OUI À LA LIBÉRALISATION
DE ÉCHANGES DE FICHIERS ...**



ARNAQUE PYRAMIDALE

Les policiers des Deux-Sèvres, en région parisienne, ont mis fin à une chaîne financière illégale de type pyramidale. Le principe est très simple. Vous recevez un courrier électronique vous expliquant que si vous apportez une certaine somme d'argent à une liste de 10 noms proposés, une fois inscrit sur cette liste vous allez recevoir 10 fois plus d'argent que votre propre ap-



port. Seulement, non seulement les chaînes pyramidales sont illicites mais surtout une belle arnaque. Neuf personnes ont été arrêtées à Bressuire, mi-mars. Ils annonçaient qu'il suffisait d'envoyer 10.000 euros pour en recevoir, ensuite, des dizaines d'autres milliers

d'euros. La centaine de participants n'a jamais rien reçu. Les policiers ont saisi 260.000 euros aux domiciles des arnaqueurs.



MOVIES 2IPHONE

Les utilisateurs de l'iPhone peuvent dorénavant installer toutes leurs vidéos sur le téléphone d'Apple. Un programme gratuit, du nom de Movies2iPhone, permet de convertir n'importe quelle vidéo (Divx, Xvid, avi, mpeg, wmv, asf, mov, ...) en un format optimisé pour l'iPhone ou l'iPod Touch. La nouvelle version sortie en mars propose aussi une gestion des sous-titres très pratique. Un petit programme freeware qui a tout d'un grand. L'auteur annonce que sa prochaine version permettra de convertir plusieurs vidéos en une seule fois. www.movies2iphone.com

BIENVENUE CHEZ LES CH'TITS PIRATES

13 Mars, quelques semaines après la sortie du film *Bienvenue chez les Ch'tits* de Dany Boon une copie pirate du DVD a été diffusée sur le web. Le pirate a signé Dany et se moque du studio Pathé en le remerciant pour ce DVD. Le pirate n'a pas cloné directement le DVD, il n'a récupéré que le film qu'il a ensuite diffusé dans les réseaux warez avant que la copie ne finisse sur le P2P.

LE PENTAGONE PIRATÉ, L'ONCLE SAM AVOUE

Juin 2007, un pirate visite un des serveurs du Pentagone. A l'époque les militaires indiquaient que l'intrus n'avait pas pu accéder à des données sensibles. Dix mois plus tard, changement de ton. Le ou les pirates informatiques ont dorénavant volé une «quantité importante» d'informations. Certaines de ces données étaient «d'une valeur stratégique» selon un

porte-parole du Département de la Défense US, Dennis Clem. Le ou les pirates avaient injecté un code malicieux qui ne sera pas détecté tout de suite. Il faudra attendre deux mois pour que les militaires se rendent compte de l'intrusion. La remise en état aura coûté 4 millions de dollars.





BOMBERMAN SUR YOUTUBE

Youtube cache dans ses dizaines de milliers de vidéos des images qui mériteraient d'être filtrées. Nous avons découvert une vidéo montrant 2 hommes, le visage masqué, en train de préparer un attentat. L'un des hommes est aidé dans la pose du bombe sur son corps. Alors qu'on nous tance les oreilles sur des filtres pour contrer les pirates de films, il serait bien de filtrer, ce type de vidéo largement plus dangereuse que la diffusion d'une daube d'Hollywood.

DÉTONNANT !

Trois fans de jeux vidéo et plus précisément de jeux musicaux comme In The Groove (Around The World) de l'éditeur Roxor Games, ont sorti une vidéo sur Youtube de folie. Jer, Nicobest et Wister, des pros de ce type de party game s'amuse à danser, avec ordinateur et tapis de danse, un peu partout (Lille, Paris, Annoeullin, piscine, gare, ascenseur, cabine téléphonique, ...).



Autant le dire tout de suite, ils ne dansent pas, ils volent, ils sautent, sans se coincer les genoux ou se péter les chevilles. Du grand art numérique. A côté, la tektonik, c'est une danse du 3ème âge. Bref, trois grands malades, mais il faut bien l'avouer, on adore ça. http://www.dailymotion.com/video/x4lj2o_in-the-groove-around-the-world_fun

LES HACKERS ONT DU COEUR

Un petit coup de pouce pour une idée super originale lancée par des artistes du nord de la France. Sirouy (un clown) et un DJ (Happy) viennent de sortir un CD quatre titres pour faire découvrir aux enfants les petits gestes simples afin de sauver la planète.



Des sons actuels, des paroles simples et des arrangements à la Bob Sinclar.

C'est vendu 5 euros. www.sirouy.fr

RUPERT MURDOCK SE FAIT CYBER-SQUATTER

Nous aurions pu le penser plus malin ou mieux conseillé le grand patron des media Rupert Murdoch. En février, le grand pont de la TV US annonçait la création d'une nouvelle chaîne de télévision Fox Business Network. Seulement, il aurait été plus intelligent d'enregistrer les noms de domaine avant de

communiquer le nom de cette future chaîne. Bref, des internautes ont sauté sur l'occasion et ont acheté toutes les adresses internet (foxbusinessnetwork.com, ...). Les avocats de Rupert Murdoch ont tenté de récupérer les adresses via une plainte au WIPO, l'organisation en charge de la propriété intellectuelle mondiale. Le WIPO n'a rien pu faire, Rupert risque de sortir la valise à billets pour récupérer les urls.

FoxBusinessNetwork.com
State of the art internet business - networking - promotion

Make money now with the HOTTEST reseller plan going

Start for only **\$90.00 PER YEAR!**

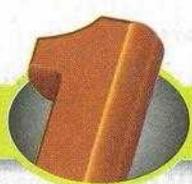
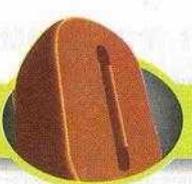
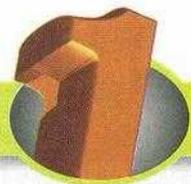
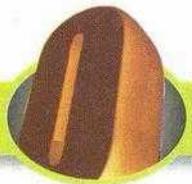
All Inclusive Reseller Plan!
- Rent Free Office, Support & Value
- Free Bonus Software
- No Deposits or Revenue Sharing

Choose the plan that's right for YOU!

| | |
|---|--|
| Basic Reseller Just \$90.00/yr! | Pro Reseller Just \$179.00/yr! |
|---|--|

FREE with Every Plan:

- FREE Traffic Package
- FREE Google Email Forwarding
- FREE Google Site Certificate
- FREE Google Site Builder
- FREE Google Email Account
- FREE Google AdWords Credit
- FREE Google AdSense Credit
- FREE Google Analytics
- FREE 24/7 Support for you and, naturally, for your customers!
- FREE 30-day Money Back Guarantee
- FREE Quick Start Marketing Guide



HOT NEWS

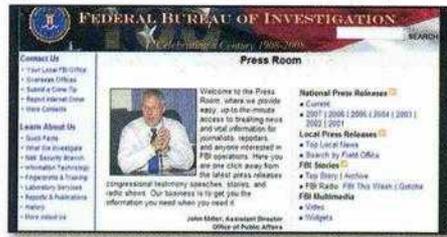
ESPIONNAGE DANS UN INSTITUT DE RECHERCHE FRANÇAIS

L'institut de recherche de la faculté de Versailles aurait eu de la visite, en février, dans un de ses ordinateurs. Dans la nuit du 10 février, une intrusion a été détectée dans l'Institut Lavoisier, spécialisé en chimie. Un ordinateur portable aurait été manipulé vers 2 heures du matin. L'école a fait appel à la DST, les services de contre-espionnage Français, pour savoir si un 007 est passé par là pour voler les secrets contenus dans la machine.



ÉCOUTE SAUVAGE DES INTERNAUTES

Robert Mueller, le directeur du F.B.I a avoué que la police fédérale avait collecté des informations sur les courriels et les habitudes des internautes américains sans l'accord d'un juge. Il a indiqué que cette espionnage était la faute des Fournisseurs d'Accès à Internet. Ces derniers auraient fourni «Trop d'informations. Nous nous engageons à agir correctement, mais également à maintenir la confiance vitale du peuple». Le FBI aurait changé de méthode depuis un an.



DES PIRATES AU CEBIT DE HANOÏRE

La police et les Douanes Allemandes se sont invitées sur les stands du plus grand salon du monde dédié aux nouvelles technologies, le CeBIT de Hanovre. Une descente très ciblée, elle visait une cinquantaine de revendeurs accusés de contrefaçons. Plus de la moitié de ces exposants étaient asiatiques: Chinois (24 stands) ou Taiwanais (12 stands). Soixante-huit caisses de preuves (lecteurs Mp4, Cdrom, DVD, ...), documents, publicité et autres gadgets ont été saisis.



Un radio Belgique piratée

Des dizaines de podcats détruits, le serveur détérioré, des backdoors cachées un peu partout. Le pirate qui est passé sur le site de la radio belge Zone80 a oublié ce

que voulait dire le mot discret. La radio n'a pas pu émettre, sur Internet, durant tout un week-end. Un acte rapidement corrigé mais qui aurait pu faire perdre des mois de travail.

PÉDOPHILES ARRÊTÉS, DES PIRATES AURAIT DONNÉ UN COUP DE MAIN

Une opération de police a permis d'arrêter un vaste réseau pédophile. Plus de 400,000 images et vidéos ont été diffusées par quatorze américains et des internautes basés en Australie, Canada, Allemagne et Angleterre. Ils se seraient fait piéger par un agent se-

cret américain infiltré dans cette organisation qui utilisait la stéganographie pour cacher les images. Des hackers auraient donné un coup de main pour casser certaines protections.



OPÉRATION CYBER-STORM II

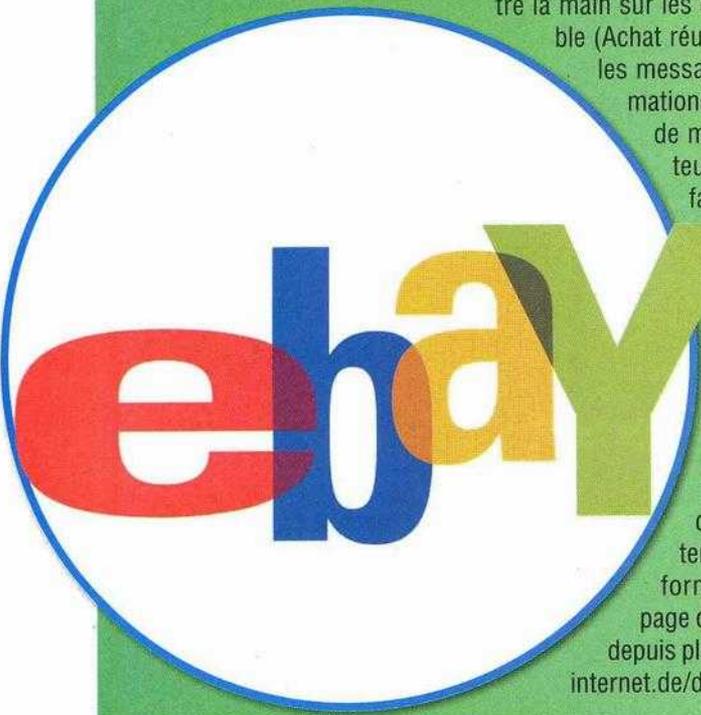
Les militaires américains, Anglais, Australiens, Néo-Zélandais et Canadiens ont participé, mi-mars, à une grande manoeuvre numérique.

Baptisée Cyber-Storm II (orage cybernétique), cette guerre numérique fictive a duré une semaine. Le scénario, des pirates informatiques ont tenté d'infiltrer des sites web, mèls, téléphones, ...

HOT NEWS

PROBLÈME SUR EBAY, UN GROUPE DE HACKERS LE PROUVE

EBay, un excellent service Internet pour vendre et acheter aux enchères. Seulement, eBay n'est pas parfait et les clients peuvent s'en rendre compte s'ils ne prennent pas quelques précautions. Des pirates peuvent accéder aux identifiants des membres du site grâce à une vulnérabilité qui n'a pas été corrigée par le site américain. Le simple fait d'ouvrir une page d'enchère eBay suffit. «En insérant un appel à un applet flash, explique les experts de Falle-Internet.de, dans le descriptif de l'annonce, il est possible par le biais du Cross-Site-Scripting (CSS) d'avoir un aperçu de toutes les données dans - mon eBay -, alors qu'elles ne devraient être accessibles qu'au titulaire du compte. En plus des informations de connexion du client, le pirate peut mettre la main sur les dernières activités de sa cible (Achat réussi/raté, liste des suivis, lire les messages privés)». Autant d'informations qui permettent aux pirates de mettre la main sur des acheteurs/vendeurs. «La faille CSS facilite aussi l'hameçonnage, confirme Falle-Internet. En manipulant certains des éléments de la page, il est possible de soumettre à la victime un faux accès login. Le mot de passe saisi sera envoyé instantanément aux pirates. Un piège qui ne nécessite aucun renvoi sur une page externe. Il suffit d'insérer le faux formulaire directement dans la page d'enchère.» eBay est prévenu depuis plus d'un an ! http://www.falle-internet.de/de/html/pr_exme_fra.php



LE CDC IS BACK

Le CULT OF THE DEAD COW (cDc), groupe mythique de hackers, propose depuis peu le système Goolag Scan, un scanner de site Internet qui utilise des commandes de recherche un peu particulière que propose Google. Son code source est ouverte sous la licence GNU Affero. www.goolag.org

LA CENSURE SUR L'INTERNET CHINOIS PAS SI EFFICACE

Edison Chen, star du cinéma chinois, présent dans le prochain Batman, a eu un problème avec son ordinateur portable. Il va donc l'amener en réparation. Quelques jours plus tard, des photos pornos d'Edison Chen avec

des chanteuses et actrices connues se sont retrouvées sur la toile. La police Chinoise, qui pourtant surveille le web avec des milliers d'hommes chargé de ce filtrage, n'a



rien pu faire. Un scandale qui a obligé Edison Chen à fuir au Canada. Il faut dire aussi que l'acteur doit se marier avec la nièce du magnat des médias Albert Yeung, le patron de Emperor Entertainment Group (EEG), connu pour ses liaisons avec les triades.



WORLD OF WARCRAFT: l'or des pirates

Neuf millions d'adeptes de World of Warcraft comptabilisés en juillet dernier. 300.000 nouveaux combattants depuis sont arrivés sur Azeroth

par Damien B.



Le business autour de World of Warcraft ne cesse de prendre de l'ampleur. Les millions de dollars qui se font via ce jeu en ligne persistant attirent bien des convoitises et les dérives mercantile de World of Warcraft. Aujourd'hui, pour ce jeu de rôle en ligne pour les communautés massivement multi-joueurs (Massively Multiplayer Online Role-Playing Games – MMORPGs), tout est à vendre pour devenir le plus puissant. Un vrai trafic est né autour de ce jeu, souvent orchestré par des groupes très efficaces

ce et particulièrement bien organisés. Des sociétés se sont même montées pour revendre des personnages, épées magiques, pièces d'or et autres items. Des sites web comme lge.com ou encore igxe.com (serveur basé en Chine, à Hong-Kong) revendent, par exemple, des pièces d'or au joueur ne souhaitant pas passer des jours et des jours à jouer. Pour 35 dollars, l'internaute reçoit 700 pièces virtuelles. Les plus tricheurs peuvent acquérir 25.000 pièces d'or virtuelles pour plus de 1.200 vrais et beaux billets verts. «Il y a beaucoup d'argent à se faire, confirme Pascal, un joueur Canadien, il suffit d'être organisé». Une organisation que certains pirates ont très vite mis en place.

:: Ferme de joueurs

Les Chinois, toujours à la pointe de l'exploitation humaine pour faire de l'argent, ont mis en place des «Game




 Here is a screenshot of my level 70 hunter. I hit level 70 the first week the Burning Crusade came out.
 You can read my all about my journey with my hunter on our site and find out all the new tricks in the Burning Crusade as I do.
Did with Confidence

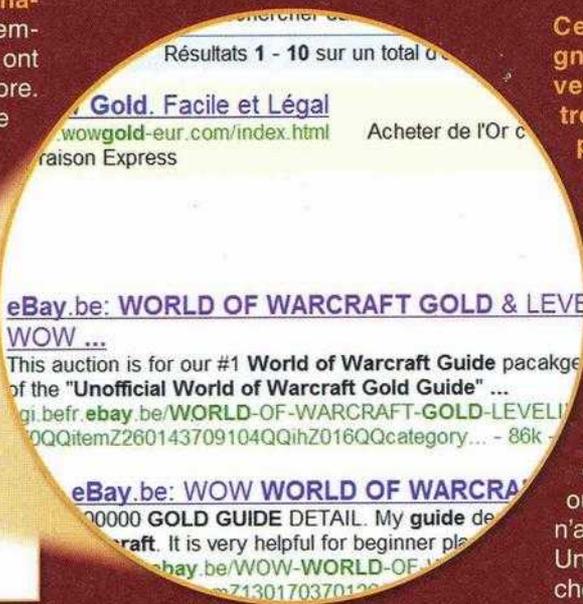
▲ **Monstre gagné à la sueur de la souris ? Non ! Acheté via Paypal.**

farming», des entreprises qui n'ont qu'un seul but, créer des personnages, des avatars. Pour cela, ils emploient des dizaines de joueurs qui ont pour mission de jouer, et jouer encore. De l'élevage électronique en quelque sorte. «Il existe aussi des groupes d'internautes, explique Pascal, qui bossent de la sorte dans les pays de l'Est. Les Roumains sont assez bien calés dans le sujet».



▲ **eBay propose des dizaines d'objets à la vente.**

L'argent semble couler à flot pour ses revendeurs, Star Wars Galaxies, Dark Age of Camelot, Everquest II, Lineage II, Guild Wars, Final Fantasy, Lord of Ring Online, et beaucoup d'autres servent de support à des ventes pourtant interdites par les éditeurs. Il est d'ailleurs intéressant de lire certains messages laissés par ces revendeurs (wowgold-eur.com), sur leur propre site de vente : « Information de livraison



: Pour la sécurité et le confort de nos clients, nous allons faire un échange de gold en ligne, en face à face. Après avoir payé vos wow gold, contacter notre support online. Dans 80-90 % des commandes, nous pouvons collectons les golds pendant la conversation. » Étonnant !

«Certains joueurs s'en moquent de payer, confirme Pascal, Dans ces mondes virtuels ils sont enfin quelqu'un. Et si en plus ils peuvent être forts et puissants. Ils sont heureux».

Blizzard tente de contrer ses joueurs à la puissance inhumaine, au point de faire des erreurs. En mars 2006, un joueur français de haut niveau se faisait jeter par l'éditeur pour avoir affiché de trop bon résultat. D'après Blizzards son statut était impossible à atteindre seul, sans une petite aide. En octobre 2005, Greg Hoglund, un internaute amateur de WoW annonçait, preuve à l'appui (<http://www.rootkit.com/blog.php?newsid=358>) qu'il avait découvert un problème d'espionnage dans WoW. Une fonction dans le jeu, baptisée Warden Client, permettait à l'éditeur de savoir qui était capable de tricher. Un spyware qui scannait et analysait, toutes les 15 secondes, les millions de machines ou était installé World of Warcraft.

:: Guerre entre revendeurs

Certains sites de revente ont pignon sur rues. Sans parler des revendeurs sur eBay, de vraies entreprises dédiées se sont montées pour ce type de vente. En Corée du sud par exemple il existe ItemMania, ItemBay et Item Play. L'année dernière ces trois sites web coréens spécialisés dans la revente d'argent, et autres articles virtuels, se retrouvaient hors ligne à la suite d'une attaque du type DoS. A l'époque, le Ministère de la Culture du pays estimait les pertes à près de 900 millions de dollars. Attaque de concurrents... ou de joueurs mécontents ? La police n'a jamais remonté la piste des pirates. Une guerre qui fait surtout des victimes chez les joueurs. MicroWorld Technologies annonçait, en 2006, avoir découvert un cheval de Troie qui avait pour mission de récupérer les identifiants



▲ **Les revendeurs proposent même des promotions.**

| SERVER LIST | |
|---------------------|------------------|
| Aegwynn Alliance | Aegwynn Horde |
| Aerie Peak Alliance | Aerie Peak Horde |
| Agamaggan Alliance | Agamaggan Horde |
| Aggramar Alliance | Aggramar Horde |
| Ahn'Qiraj Alliance | Ahn'Qiraj Horde |
| Ai'Akir Alliance | Ai'Akir Horde |
| Alextrasza Alliance | Alextrasza Horde |
| Alleria Alliance | Alleria Horde |
| Alonsus Alliance | Alonsus Horde |
| Aman'Thul Alliance | Aman'Thul Horde |
| Ambossar Alliance | Ambossar Horde |
| Anachronos Alliance | Anachronos Horde |
| Anetheron Alliance | Anetheron Horde |

PROMOTION SERVERS

Please read the **Trade Process** first



be delivered within 30 minutes!

- | | | |
|-------------------|---------------------|------------------------------|
| Ambossar Alliance | Anachronos Alliance | Bronze Dragonflight Alliance |
|-------------------|---------------------|------------------------------|



Hot servers !

- | | | |
|----------------------|--------------------|---------------------|
| Arathor Alliance | Aszone Alliance | Aszone Horde |
| Azjol-Nerub Alliance | Azjol-Nerub Horde | Eonar Alliance |
| Hellfire Alliance | Skullcrusher Horde | Wildhammer Alliance |



Super price!

- | | | |
|------------------------|--------------------|-------------------------|
| Agamaggan Horde | Aggramar Alliance | Burning Legion Alliance |
| C'Thun Alliance | C'Thun Horde | Daggerspine Horde |
| Emerald Dream Alliance | Emeriss Alliance | Frostwhisper Alliance |
| Hellscream Alliance | Illidan Horde | Khadgar Alliance |
| Kul Tiras Alliance | Moonglade Alliance | Proudmoore Alliance |
| The Maelstrom Alliance | Turalyon Alliance | Vek'nilash Alliance |
| Vek'nilash Horde | Ysondre Alliance | |



User Login

Email Contact email address

Password

Log in

Register? Why Register?
Forgot password?

SERVICE

LIVE HELP
Easy way to get answers you need

Have question with your orders?

POST YOUR QUESTION

Send us an Email

Read our Frequently Asked Questions

Tous les MMORPGs sont touchés par ces ventes. Ici, Final Fantasy XI.

de connexion (login et mot de passe) des comptes des joueurs. Autant de possibilité pirate afin de faire main basse sur les avatars électroniques et les revendre aux plus offrants. Pour contrer les ventes, les éditeurs ne peuvent rien faire. Bilan ils se rabattent sur les « tricheurs ». Décembre 2006, plus de 100,000 joueurs étaient ef-

facés des serveurs de World of Warcraft. Pour éviter les dérives, d'autres maisons de production préfèrent la méthode douce. Pour Everquest, par exemple, Sony a préféré mettre en avant les échanges entre joueurs. Ce qui n'empêche pas certains revendeurs à commercialiser des objets et autres items. Fin novembre 2007,

Blizzards mettaient en place une nouvelle sécurité. Les serveurs permettant de jouer à World of Warcraft (<http://onwarden.blogspot.com/2007/11/storm-is-brewing.html>) s'assurent, via des «check-up» permanent, qu'aucun programmes tiers (crack, trainers, ...) ne perturbent le bon fonctionnement des parties. La dernière version de ce «check» est dorénavant chiffré, codé, illisible pour les utilisateurs. Parfait pour contrer les tricheurs. Seulement ce «check-up» est dorénavant camouflé par un chiffrement. Impossible, savoir ce qui se passe entre les serveurs de WoW et vous. Rassurant ?

Les MMORPG (Massive Multiplayer Online Role Playing Game) attirent des joueurs de plus en plus nombreux. Ils attireront autant de pirates et revendeurs. Les «Gold Farmers» pullulent. On les reconnaît pourtant de loin. Ils tuent de très grandes quantités de monstres afin de collecter un maximum de pièces d'or, des items et autres objets rares. Ils n'ont plus qu'à les revendre. « Les profits sont suffisamment substantielles pour continuer, va nous confirmer Pascal, et tant qu'il y aura des acheteurs, les revendeurs continueront à rouler sur l'or ».

Ou encore Lineage 2. Des sites tenus par des groupes mafieux chinois.

CACHEZ TOUT !

Des fouineurs cherchent toujours à mettre la main sur vos données. Or certaines d'entre elles doivent absolument rester confidentielles. Voici donc un programme simple et fonctionnel !

Son nom ? TrueCrypt (www.truecrypt.org). Il s'agit d'un programme opensource qui utilise les tout derniers systèmes d'encryptage et ce, pour garantir une haute protection à toutes vos données.

:: Volume encrypté

Le système choisi par les créateurs de TrueCrypt est extrêmement simple et pratique : vous pouvez en effet créer des fichiers encryptés de la taille que vous souhaitez. Une fois activé avec le mot de passe que vous aurez paramétré lors de sa création, chaque fichier est affiché comme un volume normal, dans lequel vous pouvez copier les fichiers et documents que vous souhaitez cacher face aux regards indiscrets. Le tout est protégé par l'un des systèmes d'encryptage mis à votre disposition (il en existe au moins 8), en garantissant ainsi une sécurité maximale.

:: Aucun point faible !

Le plus agaçant avec les logiciels d'encryptage, c'est qu'ils sont très visibles ! Ainsi, toute personne s'asseyant devant votre ordinateur, peut s'apercevoir que vous disposez d'un logiciel d'encryptage parmi tous vos programmes, en l'incitant donc à chercher et trouver vos fichiers encryptés sur



CRÉEZ UNE UNITÉ ENCRYPTÉE



1. NORMAL OU CACHÉ
Cliquez sur le bouton Créer un volume. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique Créer un volume TrueCrypt standard. Pour en créer un caché, un volume standard doit en effet déjà être présent sur votre PC.



2. CRÉEZ LE FICHER
Cliquez sur Suivant et Sélectionner le fichier pour créer le fichier qui comprendra les données encryptées. Cette procédure permet de paramétrer une extension de votre choix. Sur Windows, elle apparaîtra toutefois comme valide.



3. CODAGE ET TAILLE
Les étapes suivantes vous permettent de choisir le système d'encryptage. Si vous souhaitez camoufler votre fichier en le faisant passer, par exemple, pour un film, évitez de choisir un "chiffre rond". Cela paraîtrait suspect.



4. DERNIÈRE ÉTAPE
Procédez à présent au paramétrage du mot de passe : essayez d'utiliser des lettres de l'alphabet, des chiffres et des caractères spéciaux. Terminez l'opération en cliquant sur la commande Formater.

vos fichiers. Pour peu que le fouineur dispose d'un programme spécialisé, et vous voilà dans de beaux draps ! Car ce dernier peut également parvenir à percer le codage. Pour éviter ce désagrément, il faut généralement paramétrer de longs mots de passe également composés de caractères spéciaux et de chiffres. L'utilisation d'un mot de passe de ce style déconcerte même les softwares les plus puissants en ralentissant et en compliquant l'opération. TrueCrypt surmonte facilement ce problème. Les fichiers créés peuvent en effet utiliser une fausse extension, par exemple AVI ou MPEG, pour masquer leur présence et donc protéger davantage vos données.

:: Sous menace...

Malheureusement, il faut également tenir compte des éventualités extrêmes lorsqu'on pense à la sécurité des données présentes sur nos ordinateurs. Vous pourriez par exemple être contraints de révéler votre mot de passe de décryptage sous la menace.

Volume (Volume caché) que vous devez absolument utiliser.

Concrètement, il s'agit d'un petit jeu semblable à celui des poupées russes : après avoir créé un volume normal encrypté, le programme crée un second fichier encrypté à l'intérieur de celui-ci. La lettre assignée sera la même, mais vous devrez paramétrer deux mots de passe différents.

:: ... sain et sauf quoi qu'il en soit !

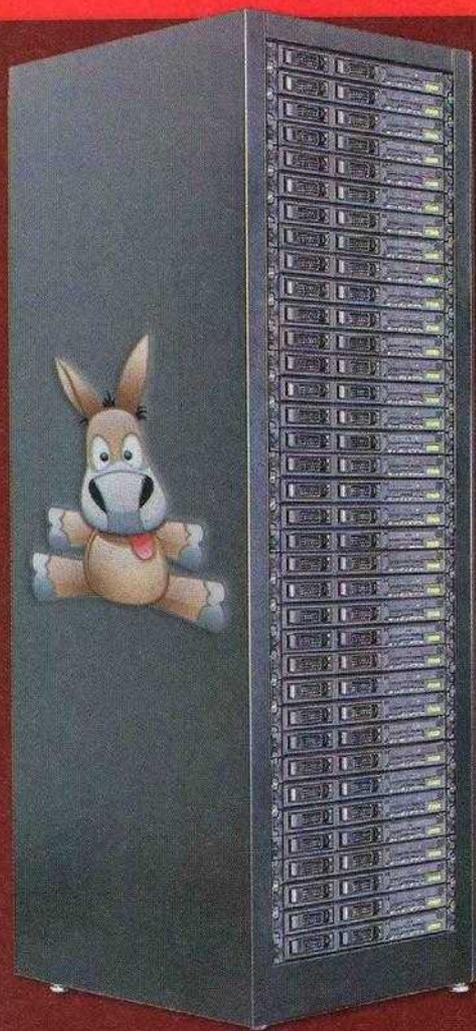
Lorsque vous sélectionnez le volume pour l'activer, le programme vous demande le mot de passe d'accès. Selon le mot de passe que vous tapez, TrueCrypt activera l'un ou l'autre fichier. Ainsi, vous pouvez insérer des documents factices ou inutiles dans le fichier principal, tandis que ceux réellement importants seront enregistrés dans le second fichier, caché à l'intérieur du premier. Si jamais vous êtes contraints de révéler le mot de passe, vous pourrez alors désigner celui qui active le fichier "inutile" : le programme ouvrira le volume normalement, sans le moindre indice d'une quelconque présence d'un second volume.

ASTUCE

Des chiffres et des lettres

Les programmes dont se servent les pirates informatiques pour percer les mots de passe, utilisent des Dictionnaires de mots courants, grâce auxquels ils parviennent à découvrir les mots d'accès beaucoup plus facilement. Pour leur rendre la vie impossible, vous devez insérer des chiffres et des caractères spéciaux dans votre mot de passe. Pour éviter qu'il ne soit trop difficile à retenir, vous pouvez utiliser une astuce très simple : remplacez certaines lettres par des chiffres ou symboles qui leur ressemblent. Ainsi, par exemple, le mot de passe framboise, peut être écrit fr4m-b0is3. Vous n'aurez donc aucun problème à vous en souvenir et parallèlement vous barrerez la route aux éventuels fouineurs.





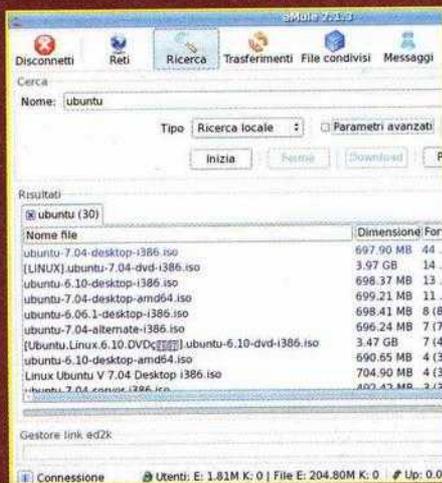
Un serveur EDONKEY pour tous !

Activez un serveur edonkey/emule dans votre réseau LAN, pour partager des fichiers en toute sérénité...

D' Une solution fiable, certes... mais c'était sans compter la déferlante du Peer-to-Peer qui a changé les habitudes et les attentes des utilisateurs : le simple échange de fichiers est devenu partage, tandis que les systèmes de messagerie internes aux programmes de P2P ont ouvert une véritable dimension sociale aux simples opérations de download et d'upload. Voyons donc comment installer un serveur edonkey/emule sur une machine du réseau local : les utilisateurs des PC de ce réseau pourront ainsi partager des fichiers (en respectant les lois sur le droit d'auteur, bien sûr...) et échanger des messages en utilisant une interface à la fois simple et familiale. Le tout, sans que le serveur et les clients eMule

ou aMule soient en contact avec le monde extérieur. Rien ne vous inter-

dit, ensuite, d'adapter les procédures indiquées à un serveur VPN.



Marre du "traditionnel" FTP pour partager vos fichiers dans le LAN ? Alors faites entrer aMule et le P2P dans votre réseau local !

:: Installation du serveur

Commencez par installer le serveur 'lugdunum' sur un ordinateur du réseau. Comme machine d'exemple, on utilisera un PC avec un système d'exploitation Linux (mais le serveur est aussi disponible pour Windows, Solaris et FreeBSD, pour ne citer qu'eux). Allez sur <http://lugdunum2k.free.fr/kitten.html> et téléchargez le binaire pour Linux i686, `eserver-17.14.i686-linux.gz`. Ouvrez une console. Le fichier est zippé, vous devez donc le décompresser à l'aide de la commande `gzip -d eserver-17.14.i686-linux.gz` et le rendre exécutable avec la commande `chmod +x eserver-17.14.i686-linux` ; créez un répertoire pour le serveur, par exemple /

usr/local/lugdunum ("mkdir /usr/local/lugdunum") et copiez à l'intérieur le fichier eserver-17.14.i686-linux.

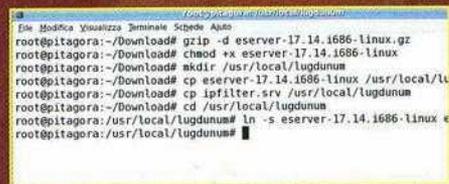
Enfin, prenez le fichier <http://lugdunum2k.free.fr/files/ipfilter.srv> et copiez-le dans le même dossier que le serveur.

:: La bonne configuration

A présent, créez avec un éditeur le fichier de configuration donkey.ini, toujours dans le répertoire où est présent l'exécutable du serveur. Tapez à l'intérieur les lignes suivantes :

```
[server]
name=Server LAN
thisIP=192.168.1.4
```

Au lieu de 'Server LAN', tapez le nom à attribuer à votre serveur emule, tandis que la variable thisIP contient l'adresse IP du serveur (elle n'est pas obtenue automatiquement par le programme). A ce stade, pour lancer le serveur, entrez dans le répertoire /usr/local/lugdunum et exécutez "./eserver-17.14.i686-linux". Par commodité, vous pouvez créer un lien symbolique dans le répertoire, comme : "ln -s eserver-17.14.i686-linux eserver"; de cette façon, pour lancer le serveur, il vous suffira d'ouvrir une console et de taper "cd /usr/local/lugdunum; ./eserver".



▲ Les étapes à suivre, depuis la console, pour installer votre serveur P2P.

Pour terminer la configuration, assurez-vous que le port du serveur emule (le 4661) ne soit pas accessible depuis Internet : dans un cadre purement domestique (un petit réseau local avec une poignée de PC connectés), il suffit généralement de laisser la configuration par défaut du routeur ADSL, où tout le trafic IP en entrée est en effet inexorablement bloqué.

Enfin, pour des raisons de sécurité, il est recommandé de lancer le serveur non pas en tant que root mais en tant qu'utilisateur commun.

:: Passez aux clients

A présent, occupez-vous des clients, c'est-à-dire des programmes (aMule ou eMule) qui vous permettront de vous connecter au serveur à partir de chaque PC connecté au réseau local. Les tests ont été effectués avec aMule 2.1.3 pour Linux, mais les instructions fournies sont facilement adaptables à son 'cousin' eMule. Tout d'abord, installez aMule (<http://www.amule.org>) sur toutes les machines : si vous utilisez une distribution Debian/Ubuntu, il vous suffira d'exécuter à partir du root "apt-get install amule" sur chacune d'elles.

A présent, suivez les prochaines étapes sur les différents PC. Lancez le programme et cliquez sur l'icône Préférences, en haut : dans la fenêtre qui apparaît, allez à la section "Connexion" et désactivez le réseau "Kademlia" ; toujours à la même section, augmentez la valeur d'Allocation Slot : de 2 ko/s, faites-la monter par exemple à 50 ko/s, de façon à pouvoir offrir davantage de bande à chaque utilisateur en upload (en cas d'utilisation du serveur emule au sein d'un réseau VPN, laissez la valeur de slot telle quelle). Puis, toujours dans la fenêtre des Préférences, entrez dans la section "Sécurité" et

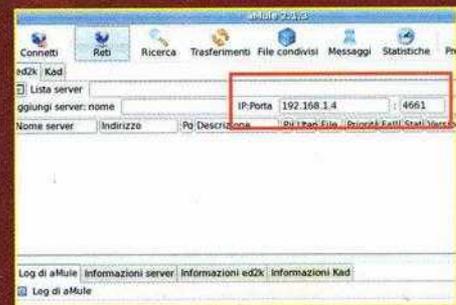


▲ Pour pouvoir vous connecter, vous devez désactiver l'option "Toujours filtrer les IP d'un LAN".

décochez l'option "Toujours filtrer les IP d'un LAN" ; dans le cas contraire, en effet, vous ne pourrez pas vous connecter au serveur local !

:: Oust les anciens serveurs, place au vôtre !

Une fois cette opération effectuée, cliquez sur l'icône "Réseaux", en haut. Si des serveurs emule externes sont présents dans la fenêtre, cliquez sur leur liste avec le bouton droit de la souris et sélectionnez la rubrique "Supprimez tous les serveurs" : ceci, pour rendre uniquement visible votre serveur privé sur les PC du réseau LAN. A présent, ajoutez ce dernier à la liste : à droite de 'IP:Port', tapez l'adresse IP de votre serveur, suivie du port sur lequel il est en écoute ; en suivant la configuration d'exemple, tapez 192.168.1.4 et 4661. Cliquez ensuite sur "Ajouter" ; une ligne apparaîtra avec les données de votre serveur : double-cliquez dessus. Ça y est, la connexion est active ! Configurez de la même façon toutes les copies d'aMule sur les autres PC du réseau. Vous pouvez maintenant partager vos fichiers et échanger des messages avec les autres utilisateurs du réseau LAN... ■

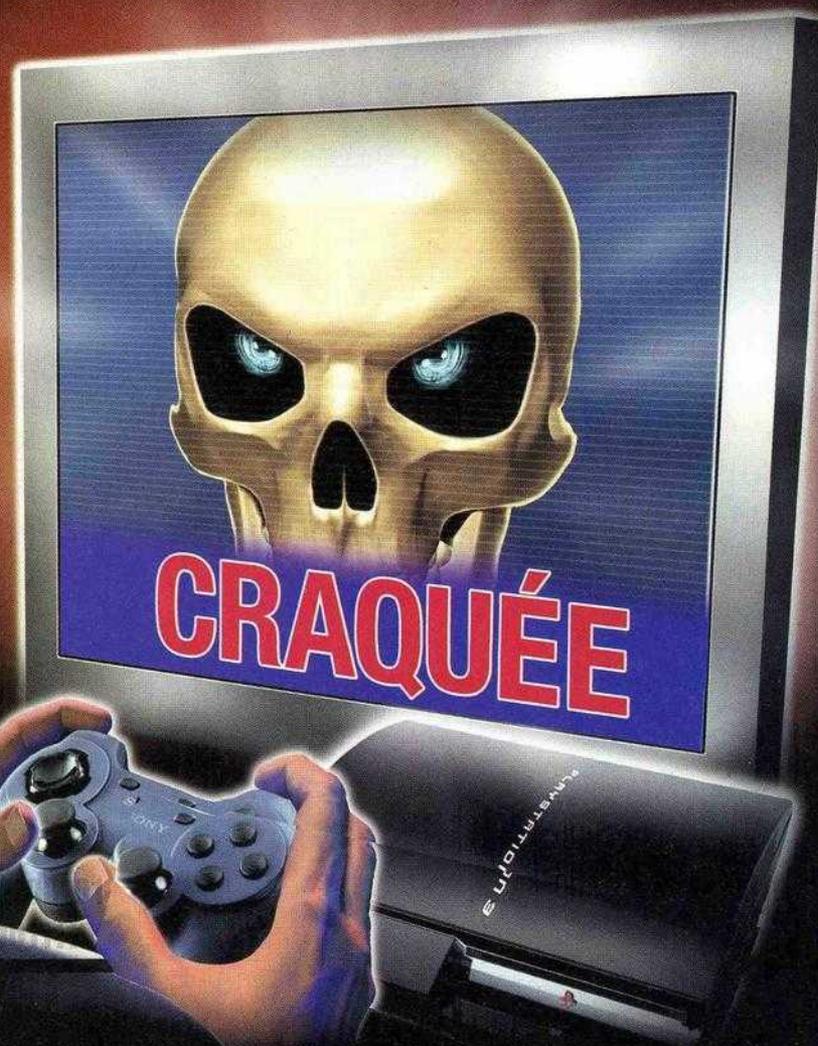


▲ Supprimez tous les serveurs de la liste, puis ajoutez l'adresse IP et le port de votre serveur privé.

M DCHIP:

Les petites puces qui démangent les consoles

Avec l'arrivée des nouvelles consoles de jeux dites de nouvelles générations, Sony, Nintendo, Microsoft en étaient sûrs. Leurs consoles de salon résisteraient aux pirates et autres bidouilleurs. Quelques mois plus tard, les puces ont envahi les salons





Quel remue ménage, dans le monde des consoles de jeux. Nous connaissons déjà les cartouches GameBoy contenant des dizaines de jeux. Les copieurs pour SNES et autres puces pour la Xbox, la PSone ou encore la Playstation II. Les constructeurs, en lançant de nouvelles machines sur le marché, ne s'attendaient pas à un tel raz-de-marais underground. Et comme dans les commerces, la grande gagnante de cette course poursuite effrénée entre bidouilleurs et éditeurs, la Wii de Nintendo.

:: Wii, l'incontournable des pirates

Avec plus de 15 puces dédiées, la Wii de Nintendo remporte la palme des puces underground, toutes consoles confondues, anciennes et récentes. C'est simple, quelques semaines après la sortie de la console de salon du géant japonais, plusieurs puces voyaient le jour. En quelques mois, les puces Cyclowiz, Cyclowiz v2, WiikKey, WiikKey clone, Wiid, Wiinja, Wiinja V2, Wiinja Deluxe, DuoWii, Wiikit, Wiifree, Wiirez, Wiisuper, ... ont permis de jouer avec des copies de sauvegardes. Une belle blague de nommer cette possibilité ainsi. Les serveurs d'échanges de fichiers regorgent de contrefaçons pour la Wii. Le business est tel que Nintendo a lancé une vague d'action judiciaire depuis le mois de septembre pour tenter de stopper les revendeurs. Fin octobre dernier, en Grande-Bretagne, un pirate informatique, Neil Stanley Higgs, alias Mister Modchips, a avoué avoir gagné en commercialisant des puces pour console plus de 1.4 million d'euros. Nintendo tente, aussi, de détruire les consoles équipées de la sorte. La sortie de Super Mario Galaxy a donné des sueurs froides aux utilisateurs de puce. La mise à jour automatique de ce jeu, mais aussi de produits comme Metroid ou encore Mario Paper, bloqué les consoles, tout simplement. Les pirates mettront quelques heures à contrer ces

attaques mais impossible de connaître la véritable impacte de ces mises à jour.

:: Xbox360, PS3, même combat

Les nouvelles consoles de Microsoft et Sony, Xbox 360 et Playstation III vont mieux résister aux assauts des pirates. Les bidouilleurs mettront un peu plus de temps à faire sauter les verrous permettant d'exploiter les potentiels underground de ces boîtes à jeu. Du moins pour la Xbox360. Six jours après la sortie dans les commerces de la Ps3 que les premières copies arrivaient sur la toile. Le groupe Paradox (disparu mystérieusement depuis, ndr) diffusait le jeu Madden NFL07. Un ISO de plus de 17 Go. Pour la machine de Microsoft, des méthodes étonnantes sont apparues, comme le flashage des lecteurs de DVD (Samsung, BenQ, Hitachi, ...). Des puces aussi, comme la Globe 360 ou encore la NME. Bref, un business juteux. Comme pour la Wii, des actions ont été lancées, sans pour autant véritablement inquiéter les revendeurs et utilisateurs. Microsoft lancera, de son côté, des actions numériques afin de bannir, du Xbox Live, les utilisateurs. Un bannissement pourtant attendu par les pirates. En 2004, Microsoft avait déjà annulé les comptes des utilisateurs d'une XBOX pucée. La mise à jour du jeu Halo leur avait été fatale. Même sanction, 3 ans plus tard, avec Halo 2. Et les bidouilleurs ne s'arrêtent pas ! Un de ces groupes de fans du fer à souder a inventé et fabriqué la première puce multi consoles. Baptisée Infectus, ce modchip est capable de fonctionner sur une Wii, une XBOX 360 mais aussi sur une Playstation 3. D'après la boutique qui commercialise la chose, La puce est livrée vierge. Elle est programmable via le port USB. «Une fois programmée elle est capable de fonctionner comme les puces GLOBE 360 ; Puce O2 et WIIFREE». Une puce commer-

LINK

Quelques sites passionnants pour suivre l'actualité des consoles de jeu et leurs petits à côté underground.

www.xavbox360.com

Tout sur la XBOX 360.

www.xavboxwii.com

L'univers de la Wii.

gueux-forum.net

Forums dédiés aux consoles de salon et portables.

gx-mod.com

Actualité sur les petits à côté des consoles (puces, HomeBrew)

www.modchip.com

Customiser sa console.

cialisée 43 euros. Totalement légale, car commercialisée vierge. Ils sont malins, quand même, ces bidouilleurs !

:: Fausses consoles

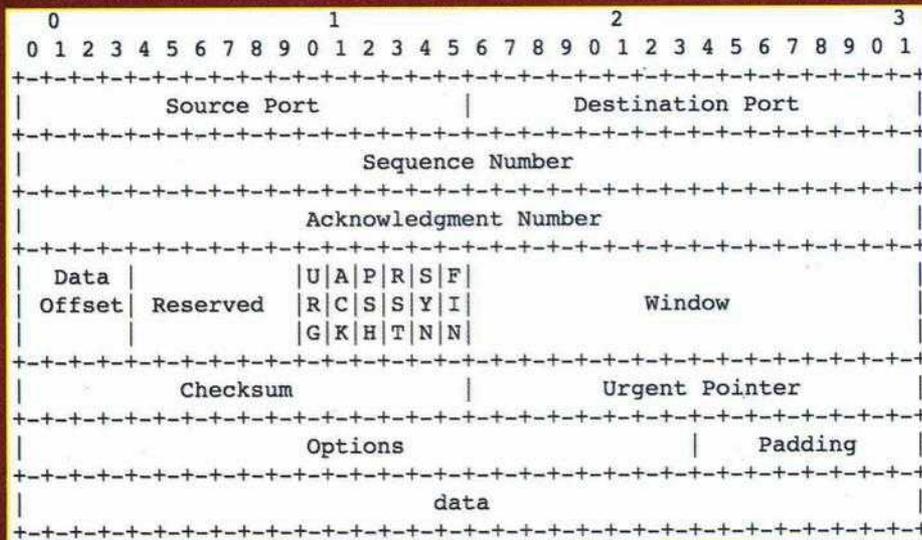
Le plus drôle, façon de parler, est que ces consoles se font pirater, aussi, par des contrefacteurs asiatiques qui ne manquent pas d'humour. Depuis quelques semaines, des consoles Vii (copie de la Wii), de FunStation 3 (copie de la PS3) ou encore POPstation (copie de la PSP) débarquent en force dans les boutiques peu regardantes sur les produits. Des machines qui reproduisent la coque, la boîte, les manettes mais cachent, dans la majorité des cas, des jeux datant des années 80. Certains lecteurs ont même aperçu des POPstation dans des loteries proposées sur des stands de fêtes foraines françaises. Pour conclure, faut-il le rappeler, les puces, comme ces copies de consoles, sont illégales en France. Contrefaçon et recel de contrefaçon peuvent coûter jusqu'à 300.000 euros d'amende et 5 ans de prison. ■



L'œil INVISIBLE

Comment effectuer le scan d'un réseau sans être repéré ? En utilisant ledit réseau pardi !

Lorsqu'un ordinateur (ou une interface) souhaite interagir avec un autre ordinateur, il doit utiliser un système appelé "protocole de communication". Un protocole n'est rien d'autre qu'un système univoque qui permet à deux systèmes ou plus de "se comprendre" et dialoguer. Les deux protocoles les plus utilisés pour les communications via Internet sont les suivants : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol). Ce qui les différencie ? Une approche différente de qualité de la communication. Ils sont donc utilisés pour des connexions fiables et performantes. Pour approfondir la connaissance du protocole TCP, nous vous renvoyons à la documentation



officielle présente à l'adresse suivante : "http://tools.ietf.org/html/rfc793".

::Schéma du TCP header

Du TCP...

En allant un peu plus loin dans le protocole TCP, on peut dire que lorsqu'un ordinateur commence à communiquer avec un autre, il envoie toute une série d'opérations préliminaires pour initialiser la session. Cette séquence de commandes est appelée "handshake". Dans la première phase du handshake, le premier ordinateur envoie un paquet au PC destinataire, en paramétrant à 1 le bit SYN du TCP header. Si le port correspondant à la demande est ouvert, l'ordinateur de destination répond alors au premier en envoyant un paquet, en paramétrant à 1 les bits ACK et SYN. Dès lors, les deux ordinateurs sont "connectés" entre eux grâce à la session TCP ouverte et peuvent donc procéder à l'échange de données en tout genre. Pour mettre ensuite un terme à la connexion, le premier ordinateur enverra au destinataire un paquet TCP avec un flag RST actif.

... au SYN SCAN

Grâce au fonctionnement du système de handshaking, un système de scan a été élaboré, capable d'exploiter pleinement cette caractéristique. Le "SYN SCAN" est justement l'une des méthodes les plus rapides, efficaces et invisibles (sans ouvrir de sessions TCP complètes, rien n'est enregistré sur les fichiers log) actuellement utilisées pour le scan de réseaux. Son fonctionnement est en effet centré sur l'envoi de paquets SYN à des ports déterminés qui, en fonction de la réponse du système destinataire, vérifient si un port est ouvert ou non. Ce système est bien plus efficace qu'un scan "standard" puisqu'il n'ouvre jamais de connexions TCP complètes qui, dans de nombreux

cas, pourraient être refusées par un firewall hardware ou software.

:: Exemples

Commençons nos tests. En lançant la commande nmap 127.0.0.1, vous devriez recevoir une réponse du style :

```
root@HomeServer:~# nmap 127.0.0.1
Starting Nmap 4.20
( http://insecure.org )
at 2007-11-17 22:56 CET
Interesting ports on localhost (127.0.0.1):
Not shown: 1694 closed ports
PORT      STATE SERVICE
80/tcp    open  http
631/tcp   open  ipp
3306/tcp  open  mysql
Nmap finished: 1 IP address
(1 host up) scanned
en 0.128 secondes
```

En moins d'une demi-seconde, le programme a contrôlé et identifié tous les ports et services relatifs, actifs sur notre ordinateur (dans notre cas, un webserver, l'Internet Printing Protocol et le démon MySQL). Rien qu'en utilisant une commande aussi simple, on parvient déjà à obtenir plusieurs informations sur la station cible. Essayons maintenant en utilisant la commande "nmap -A -sS 127.0.0.1". Le résultat ressemblera à ça :

```
root@HomeServer:~$ nmap -A 127.0.0.1
Starting Nmap 4.20
( http://insecure.org )
at 2007-11-17 23:00 CET
Interesting ports on localhost (127.0.0.1):
Not shown: 1694 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-lubuntu6)
631/tcp   open  ipp CUPS 1.2
3306/tcp  open  mysql MySQL 5.0.45-Debian_lubuntu3-log
Service detection performed. Please report any incorrect results at
http://insecure.org/nmap/submit/ .
Uptime: 0.121 days (since Sat Nov 17 20:19:20 2007)
Network Distance: 0 hops
Nmap finished: 1 IP address (1 host up) scanned in 6.251 seconds
```

En quelques secondes, grâce également à la méthode SYN SCAN (option -sS), vous trouverez même la version des différents services lancés (dans notre cas, webserver Apache version 2.2.4 [avec PHP 5.2.3], CUPS 1.2 et le démon MySQL mis à jour dans sa version 5.0.45), très utile si vous disposez de quelques beaux exploits.

Tout cela n'est qu'une infime partie du potentiel de NMAP. Il vous suffit de lancer un "man nmap" pour voir apparaître toute une documentation à n'en plus finir.

Salut à tous et bon scan !



Attention !!! Des exigences graphiques nous ont obligés à casser cette ligne de code.

MATRIX

Dans le film Matrix Reloaded, Trinity utilise Nmap pour pénétrer dans le système de la centrale électrique, à travers le forçage des services SSH et le bug CRC32 (découvert en 2001)

L'ESPION qui venait D'INTERNET

Big Brother existerait-il vraiment ? Quelqu'un vous espionne-t-il par le biais de votre PC ? Ou de votre portable ? Voici comment vous défendre face à ces menaces !

La seconde moitié du vingtième siècle a été caractérisée par une peur qui s'est généralisée, à travers un comportement qui a parfois même débouché sur des cas de véritables crises d'hystérie collective. Nous sommes tous préoccupés par le fait qu'un œil inquisiteur vienne contrôler notre identité, nos actions ou même nos pensées. Mais qu'y a-t-il de vrai dans tout cela ? Et si les choses sont ainsi, comment faire pour protéger le plus possible notre confidentialité ?

INSTALLATIONS

Echelon bénéficierait de nombreuses installations, très coûteuses, réparties dans le monde entier. Les rapports parlent en effet de plus de 50 stations d'écoute dans le monde, y compris la base aéronautique de San Vito dei Normanni, dans la province de Brindes (fermée en 1994) et d'autres bases similaires implantées en Allemagne, Espagne, Royaume-Uni, France, Danemark, Chypre, Malte, Turquie, etc.



:: Le mystère Echelon

De nombreuses rumeurs et légendes circulent sur Echelon, un supposé réseau secret international de recherche, d'échange et de traitement des informations, qui surveillerait nos moindres faits et gestes par le biais de nos ordinateurs, portables, cartes de crédit, etc.. On dit que ce réseau serait sous le contrôle de la Communauté UKUSA, elle-même dirigée par les services secrets de cinq nations anglo-saxonnes (Australie, Canada, Nouvelle-Zélande et, surtout, Etats-Unis et Royaume-Uni). Attention : il ne s'agit pas ici de simples légendes métropolitaines ! Les informations mentionnées proviennent également de rapports officiels de la Communauté européenne, comme ce fut le cas en 2001. L'existence d'Echelon a été révélée pour la première fois par Duncan Campbell, journaliste d'investigation indépendant, mais aussi producteur d'émissions télévisées, dans un article publié sur la revue anglaise *New Statesman* en 1988, intitulé *Someone's Listening* : quelqu'un écoute. Si l'on en croit cet article

SHAREWARE ET SPYWARE

On trouve aujourd'hui de nombreux programmes sharewares : ces fameux programmes qui vous proposent une période d'essai gratuite ou avec des fonctions limitées, et que vous pouvez télécharger et installer à partir d'Internet. Mais attention, car certains installent aussi automatiquement des programmes espions qui redirigent votre navigateur vers d'autres sites web, ou collectent des informations sur votre compte pour les envoyer à d'autres personnes qui vous envoient ensuite de la pub personnalisée, etc.. Parmi les programmes les plus à risque, signalons Bonzi Buddy, Dope Wars, ErrorGuard, Grokster, Kazaa, Morphheus, RedLight, WeatherBug, EDonkey2000 et WildTangent.

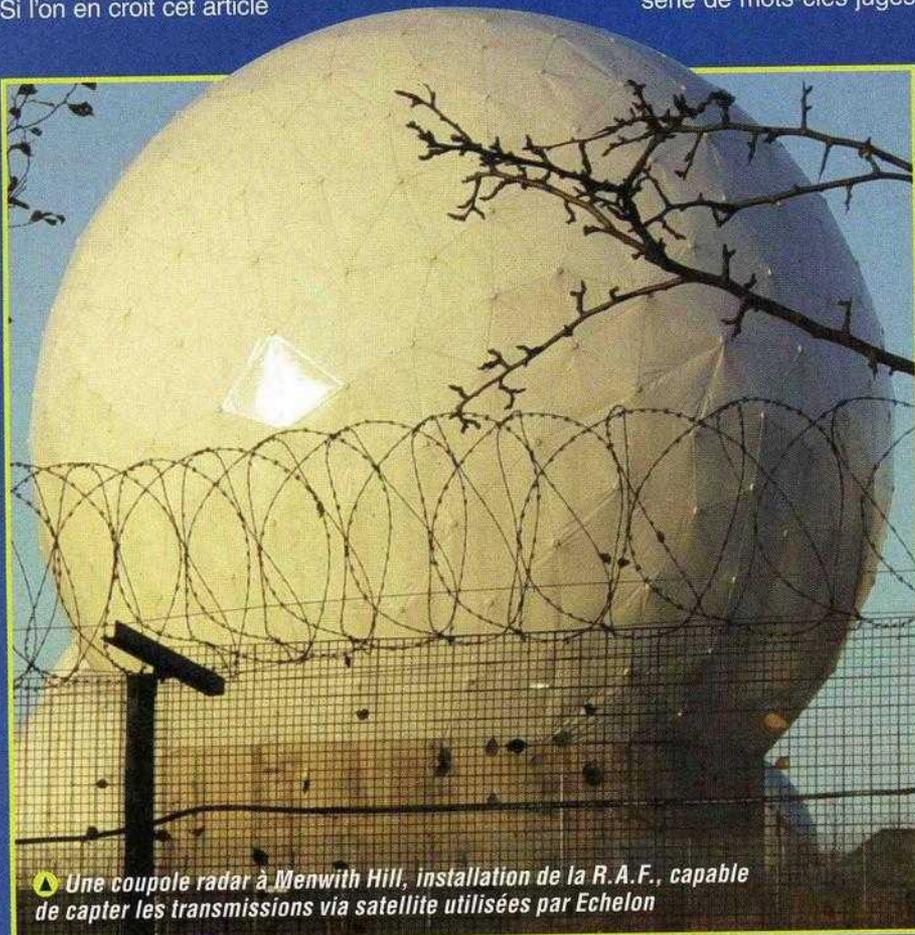


Good evening ! How has your day been!

et de nombreux autres rapports et récits provenant de différentes sources, Echelon pourrait facilement capter des communications satellites et radio, conversations téléphoniques, fax, e-mails etc., et pourrait aussi archiver chaque information reçue de façon totalement automatisée, en s'attardant uniquement sur toute une série de mots-clés jugés

dignes d'intérêt. Pour contre-balancer de nombreuses affirmations scandaleuses et souvent excessives, nous pouvons dire que le Comité de la Communauté européenne qui a enquêté sur ce phénomène et qui a publié le rapport dont nous venons de parler, a conclu que les capacités techniques d'un tel système étaient en réalité bien plus limitées que voudraient bien nous le faire croire ces "bruits de couloir". Des capacités qui semblent malgré tout assez préoccupantes, même après un bilan réaliste. Les transmissions radio à haute fréquence (également appelées ondes courtes) peuvent effectivement être interceptées facilement, même à grande distance. L'installation de satellites spécifiques pour faciliter les communications et les transmissions audio/vidéo permet de tenir un registre, mis à jour pratiquement en temps réel, de tout type de message qui passerait par ces satellites : coups de fil, fax, e-mails, trafic de données, émissions de télévision, radio et bien d'autres encore. A ce jour, toutefois, les transmissions vocales et autres transmissions de données passent à 99 % par des connexions à fibres optiques, ce qui rend l'interception beaucoup moins facile : cela nécessite l'installation de stations d'écoute sur les lignes de ces fibres optiques, et rend les capacités de contrôle d'Echelon bien plus limitées qu'il y a quelques années.

Echelon n'est donc pas une légende, loin de là, même s'il y a peu de chance pour qu'il contrôle toute la population mondiale, tel un super "Big Brother", en s'occupant uniquement des "zones chaudes" et de certains types de communication.



▲ Une coupole radar à Menwith Hill, installation de la R.A.F., capable de capter les transmissions via satellite utilisées par Echelon

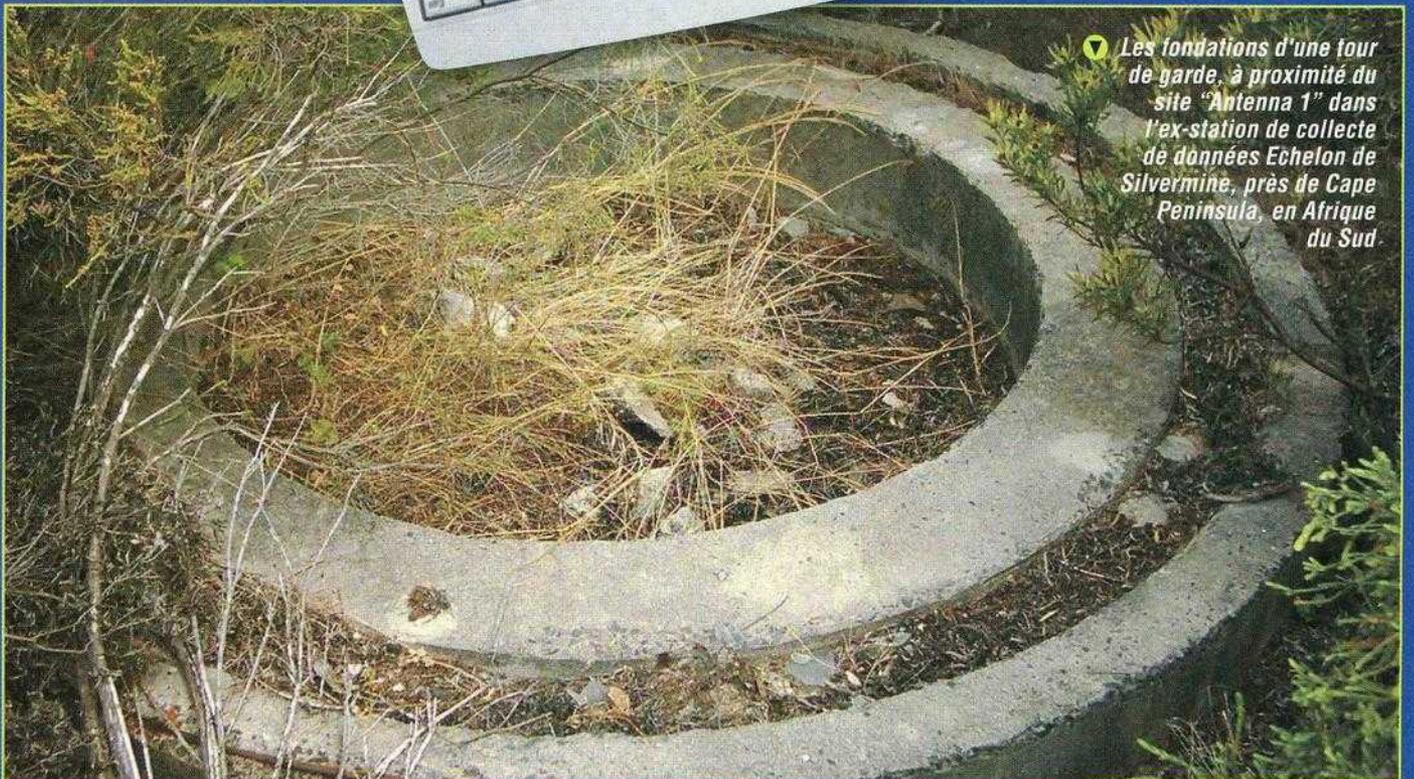
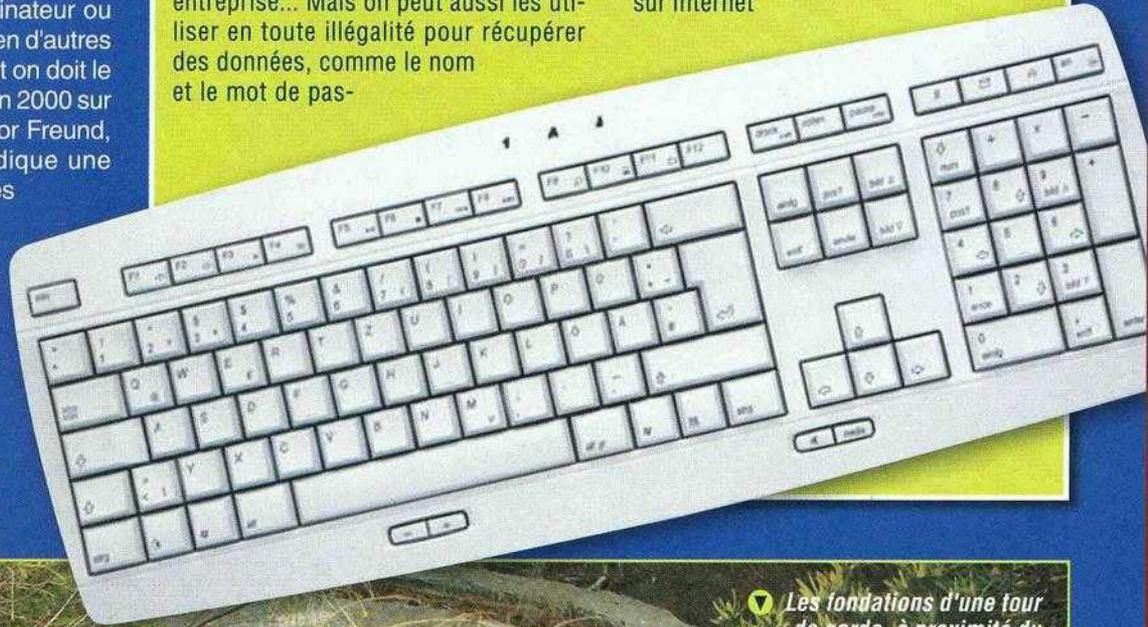
:: Programme-espion

Nous avons déjà parlé dans ces pages des spywares, ces programmes réalisés spécifiquement pour espionner vos moindres faits et gestes virtuels par le biais de votre PC fixe. Mais les spywares ne se contentent pas de vous espionner : ils effectuent aussi des actions qui peuvent être extrêmement agaçantes voire dangereuses. Ils peuvent ainsi transmettre vos données aux programmeurs sans aucune autorisation, prendre partiellement le contrôle de votre ordinateur ou de certains programmes, et bien d'autres choses encore. Ce terme, dont on doit le sens actuel à un rapport sorti en 2000 sur la sécurité et rédigé par Gregor Freund, fondateur de Zone Labs, indique une grande variété de programmes avec les fonctions les plus disparates. Selon une étude menée il y a deux ans par America On Line et par la National Cyber-Security Alliance, 61 % des ordinateurs analysés contenaient certaines formes de spywares et 92 % des détenteurs de ces ordinateurs n'étaient

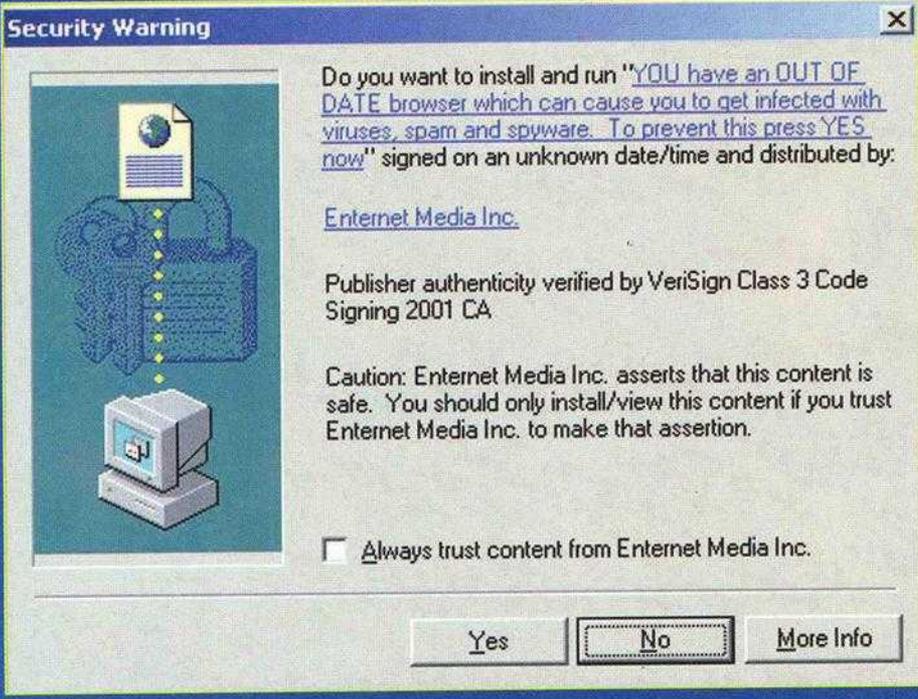
KEYLOGGER

Les programmes appelés **Keystroke Logger**, ou plus simplement **Keylogger**, sont conçus pour enregistrer toutes les touches du clavier qui sont pressées par l'utilisateur du PC infecté. Ils peuvent être utilisés de façon licite pour contrôler d'éventuelles erreurs de programmation ou d'insertion de données, ou pour garder sous contrôle la productivité des employés d'une entreprise... Mais on peut aussi les utiliser en toute illégalité pour récupérer des données, comme le nom

et le mot de passe se utilisé pour accéder à des programmes et sites Internet, de façon à permettre leur accès à l'auteur du Keylogger. De nombreux anti-spywares sont en mesure d'identifier et de bloquer ces applications et il est en outre conseillé d'avoir un pare-feu qui contrôle tous les programmes exécutés, si vous ne voulez pas vous faire voler le mot de passe de votre compte bancaire sur Internet



▼ Les fondations d'une tour de garde, à proximité du site "Antenna 1" dans l'ex-station de collecte de données Echelon de Silvermine, près de Cape Peninsula, en Afrique du Sud.



▲ Un message apparaît dans une fenêtre de votre navigateur et vous informe que votre système est infecté : ne tombez pas dans le panneau, c'est un faux anti-spywares qui va tout faire pour que vous l'installiez

pas au courant de leur présence. 91 % de ces derniers ont affirmé n'avoir jamais donné la moindre autorisation à des tiers pour installer ces programmes sur leur PC. D'après les données statistiques relatives aux rapports envoyés aux développeurs qui produisent des programmes anti-spywares, neuf ordinateurs sur dix connectés au réseau seraient infectés. Les différentes versions du système d'exploitation Microsoft Windows sont

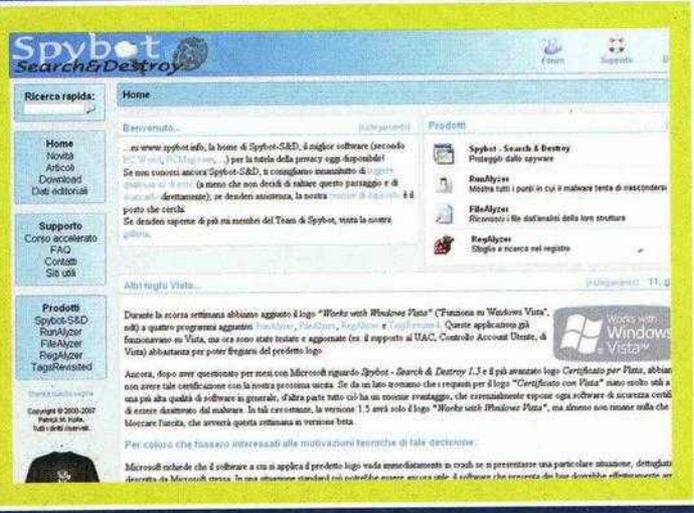
dans l'absolu les plus touchées par ces 007 virtuels, et l'utilisation d'Internet Explorer est pour eux une véritable manne tombée du ciel, puisque son intégration avec le système d'exploitation permet à ces programmes d'avoir un accès direct à des parties vitales de l'ordinateur, avec la possibilité de modifier des codes de registre et autres fonctionnalités de différents programmes et applications. Mieux vaut donc, dans la mesure du pos-

sible, utiliser un autre navigateur Internet (comme par exemple Mozilla Firefox) voire même un autre système d'exploitation (comme Linux ou, dans le cas d'un Mac, MacOS). Pour se libérer de ces infections électroniques, il est nécessaire d'installer un programme anti-spywares et de le tenir constamment à jour, en faisant attention aux sites que vous consultez et en évitant de cliquer sur des liens publicitaires ou d'installer des "barres" supplémentaires apparemment inoffensives et qui, en réalité, peuvent vous créer de sérieux problèmes. Mais les créateurs de spywares ne sont pas restés les mains dans les poches et ont lancé une grande quantité de faux produits anti-spywares qui, une fois installés, non seulement ne suppriment pas les infections présentes, mais ajoutent leurs propres infections, en s'auto-défendant face à d'éventuelles autres attaques. Si vous tombez sur une page Internet où un message vous prévient qu'un virus ou un spyware a été détecté, avec un message du style "cliquez ici pour supprimer l'infection", ne l'écoulez surtout pas ! Ces faux liens entraînent généralement l'installation de l'un de ces faux programmes anti-spywares. La liste s'allonge chaque jour, mais voici à titre d'exemple les noms de certains de ces programmes très dangereux : errorsafe, Pest Trap, SpyAxe, AntiVirus Gold, SpywareStrike, Spyware Quake, WorldAntiSpy, Spylocked, SysProtect, Spy Sheriff, Spy Wiper, PAL Spyware Remover, PSGuard, MalWare, WinAntiVirus Pro 2006, WinFixer, Spydawn et ContraVirus ■

ANTI-SPYWARE

Nombreux sont les programmes que vous pouvez utiliser pour surveiller et supprimer des spywares éventuellement présents sur votre système, ou pour faire face à des tentatives d'intrusion de différent type. Parmi les plus célèbres, notons : Ad-Aware, Bugoff, CA Anti-Spyware, CWSredder, Counterspy, Ewido Networks, Hijack

This, Hitman Pro, NoAdware, Real-time Protection, RottkitRevealer, Spy Sweeper, SpyCatcher Express, SpyHunter, SpySubtract, Spybot - Search & Destroy, Spyware Doctor, Spyware Removal, System Safety Monitor, Windows Defender, Windows Malicious Software Removal Tool, XOFtspy Portable Anti-Spyware, Zerospysware et EAcceleration



CRACKER UN MOT DE PASSE : TOUT UN ART !

Un passe-temps formellement interdit sur l'ordinateur d'autrui, presque un sport... Mais au final, quel est le plus rapide des programmes de crackage ?

Vous souhaitez savoir comment obtenir un accès administrateur sur un ordinateur Windows XP ? Alors suivez le guide... Pour cela, deux solutions s'offrent à vous : supprimer le mot de passe d'un utilisateur administrateur existant ou le trouver.

La différence est substantielle. Le premier système est simple et rapide, mais présente toutefois un inconvénient : il révèle à tous les utilisateurs du compte que le mot de passe a été violé et que quelqu'un a eu accès au système à travers ce compte. Le second système est plus complexe et ne fonctionne pas toujours à 100 %, mais il vous garantit, en récupérant le mot de pas-

se, de passer totalement inaperçu. Son propriétaire ne s'apercevra en effet d'aucun changement quant à son utilisation.

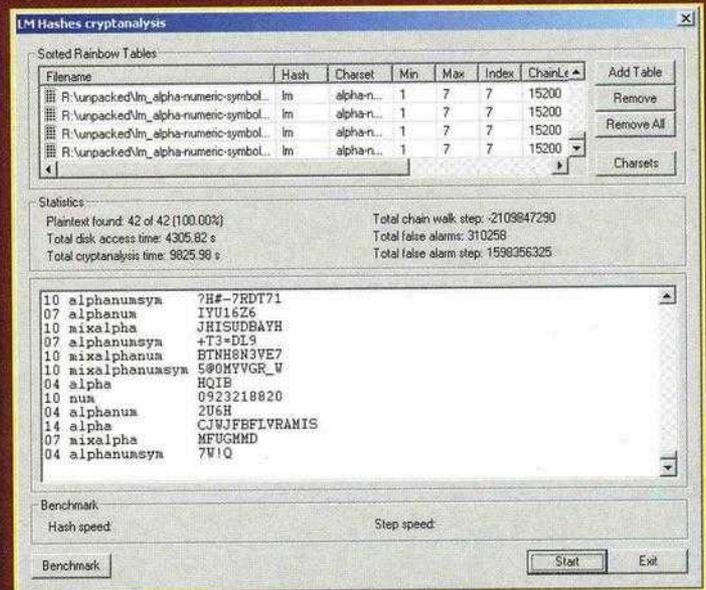
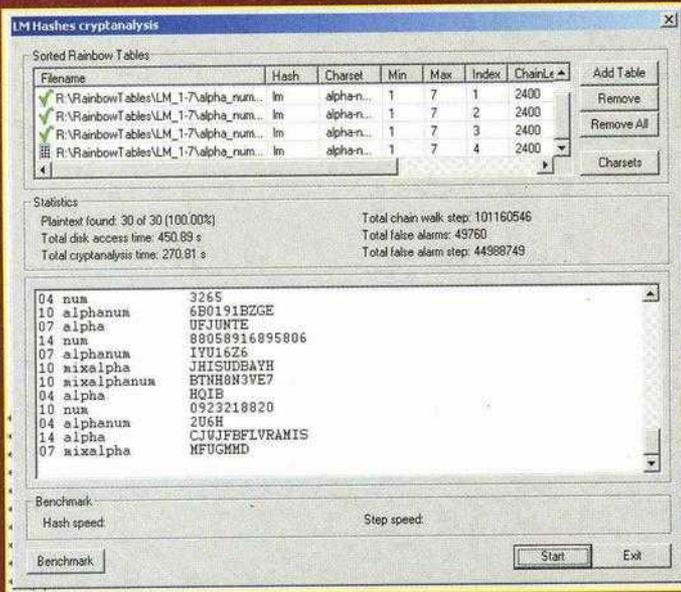
:: Hashing

Comme d'autres articles l'ont déjà traité dans HM, lors du premier accès ou de la création d'un nouvel utilisateur, le système d'exploitation enregistre un hash (littéralement "viande hachée", concrètement une empreinte digitale) de votre mot de passe. Les hashes supportés par Windows sont les suivants : LM (abréviation de LanMan) et NT-LM, une évolution du LM. En effet, tandis que le premier supporte 7 caractères maximum et ne fait pas de distinction entre les majuscules et les minuscules, le second supporte quant à lui jusqu'à 128 caractères et fait la distinction entre les majuscules et les minuscules.

XP utilise les deux, en se contentant de désactiver le LM si le mot de passe est composé de 15 caractères ou plus, tandis que Vista utilise exclusivement le système NTLM avec une sécurité moyenne nettement supérieure. Il faut dire aussi que pour pouvoir effectuer le hachage de mots de passe jusqu'à 14 caractères, XP casse le mot de passe en 2 parties de 7 caractères. Ainsi, si 'p455wordF1ga' est le mot de passe, le résultat sera le suivant :

```
DFB470CB7A366D6CEB1E89
7CA4635FBF pour le LM,
où DFB470CB7A366D6C est
le hash de 'p455wor' et
EB1E897CA4635FBF est le hash
de 'dF1ga'
2D7AFB5902034EBD28E8313F
E5E75593 pour le NTLM
```

Les deux hashes font 32 bytes, mais la différence est substantielle !!!



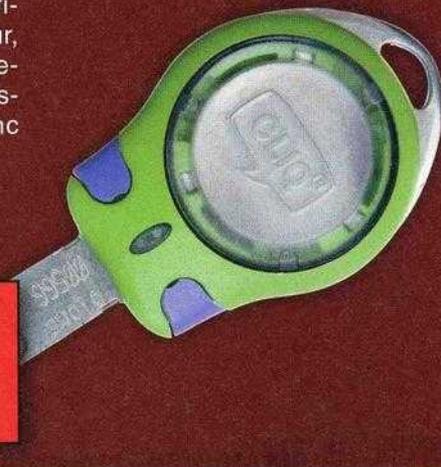
▲ Tous les mots de passe alphanumériques composés de 4 à 14 caractères crackés en 12 minutes.

▲ Tous les mots de passe alphanumériques et symboles composés de 4 à 14 caractères, crackés en moins de 4 heures.

Nous pouvons attaquer chaque sous-hash LM de 16 bytes en sachant qu'ils sont le résultat de 7 caractères maximum de mot de passe, tandis que nous ne savons absolument rien du hash NTLM. Si on n'a que le hash NTLM, on sait alors que le mot de passe est composé de 15 à 128 caractères si le hash provient de XP, tandis que si le hash vient de Vista, on ne sait absolument rien... le mot de passe pourrait être composé de 1 à 128 caractères, en contenant n'importe quel caractère UNICODE.

Ça c'est la règle générale ! Seule exception possible ? Lorsqu'un administrateur système consciencieux paramètre XP pour ne pas générer le hash LM du mot de passe, en nous donnant ainsi pas mal de fil à retordre. En réalité, il s'agit d'une modification souhaitable sur tout ordinateur, qui peut être réalisée en quelques secondes, en modifiant une clé du registre de configuration (cherchez donc sur google !).

Linux ne diffère pas beaucoup de Windows en tant que processus, mais les différences sont importantes : il utilise md5 comme algorithme de hachage et, dans la plupart des distributions, "sale" le hash en insérant une valeur aléatoire. Les anglais appellent le résultat "hash with salt" (littéralement "avec du sel"). Saler le hash signifie insérer dans le mot de passe d'origine du texte supplémentaire décidé par l'algorithme, de façon à générer des hashes totalement différents de ceux créés en effectuant le simple hachage de la chaîne d'origine. Une technique très utile contre les attaques par dictionnaire, mais nous traiterons le crackage de hash md5 un peu plus loin.



Attention !!!
 Des exigences graphiques nous ont obligés à casser cette ligne de code.

:: Ecraser le mot de passe

Revenons au cas de Windows. Retrouver le mot de passe au final ne nous intéresse plus tant que ça. Nous, ce que nous voulons c'est accéder immédiatement au système en tant qu'administrateur car nous n'avons pas la patience d'attendre ! Condition nécessaire et suffisante pour que cette opération soit possible : effectuer le boot à partir d'une unité optique. Il existe de nombreux CD et DVD live capables d'effectuer cette manip, certains basés sur Linux, d'autres sur BartPE (un Windows LiveCD).

Par exemple :
 Spotmau Password Recovery 2007 (vendu dans le commerce 19,95 US\$, PC-DOS)
http://www.spotmau.com/products/package/pw_recovery.htm
 Ophcrack 1.2.2 (free, Linux + SLAX)
<http://ophcrack.sourceforge.net/>
 Cain CD/DVD Live (free, BartPE)
<http://www.dxdive.com/cain/>

Les deux programmes free vous permettront également de tenter un crack directement depuis le CD Live, mais nous vous en reparlerons après...

Concrètement, ces CD contiennent

```

F:\WINDOWS\system32\cmd.exe
F:\bin2>psexec -s \\192.168.40.30 -c gsecdump.exe -s
PsExec v1.71 - Execute processes remotely
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Administrator(current): 500:0283527a1736f2f8d863baec9895d56b:d9514b62d442ede2e1a611a00f102138::
Administrator(hist_01): 500:0283527a1736f2f8d863baec9895d56b:d9514b62d442ede2e1a611a00f102138::
Administrator(hist_02): 500:56c3181cb75d5f3402d56b8b3a16ba56:f54a83a5b79ce6220297bd94d902cf77::
Administrator(hist_03): 500:0283527a1736f2f8d863baec9895d56b:d9514b62d442ede2e1a611a00f102138::
Guest(current): 501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
krbtgt(current): 502:aad3b435b51404eeaad3b435b51404ee:1f175b7d071a342c1b33651bab9ecec3::
s-antivirus(current): 1104:3575d13eeca6b86e37be3b1be3b25dce540ac85b5d5f75ac709994706ff39c::
arcservice(current): 1105:16ca416c2658e00daad3b435b51404ee:938df8b296dd13d0dece8aa37be593e0::
ulla(current): 1106:c350aa4028458522aad3b435b51404ee:160d4348bfbbe4001dccecd5278fe17b::
janne(current): 1107:14af091e8bab02adaad3b435b51404ee:8c27847ed8bed581b048f46078f8e77::
pelle(current): 1108:06e280a22686d96baad3b435b51404ee:3a01f0ce36685d481305a1a77f052fec::
pelle(hist_01): 1108:06e280a22686d96baad3b435b51404ee:3a01f0ce36685d481305a1a77f052fec::
pelle(hist_02): 1108:67d41137428a2a4baad3b435b51404ee:360493bc72980cf887fab89eae61aa7::
kalle(current): 1111:b267df22cb945e3eaad3b435b51404ee:36aa83bdcab3c9fdaf321ca42a31c3fc::
kajsa(current): 1112:4adb32803979b521aad3b435b51404ee:39be997333daDe66be7f853b1706a79e::
knatte(current): 1113:064399eca5e622caad3b435b51404ee:7530f1ff74d1a28a20f8e3747sec11b::
fnatte(current): 1114:6d70c7110f5e76caad3b435b51404ee:8e7cd9820936efced598a3754325d91::
tjatte(current): 1115:ff3750bcc2b22412c2265b23734e0dac:fd0896477d4e8bf81345cd4d464d381b::
arcservice(current): 1116:16ca416c2658e00daad3b435b51404ee:938df8b296dd15d0dce8aa37be593e0::
backdoor(current): 1117:499fbc7bc03a8038944e2df489a880e4:16731c9f238c5c2b4f129483fa875254::
konsult(current): 1118:31ada3adb7b6952aad3b435b51404ee:d1e4549d94812259095daa577c7ee33a::
maja(current): 1119:736a748943ecb1d7aad3b435b51404ee:3ac552113404184bf94abbe94688aaae::
marcus(current): 1120:b267df22cb945e3eaad3b435b51404ee:36aa83bdcab3c9fdaf321ca42a31c3fc::
itsupport(current): 1121:d4d7cac784102c40aad3b435b51404ee:35a0c5c8b8e7e7eeb3cb62323c7b1f73::
    
```

⚠ **Préparez-vous à des opérations assez longues surtout si vous avez choisi un mot de passe avec des caractères spécial unicode.**

un programme très simple qui localise dans les fichiers SAM de Windows (c:\\$windir\$\system32\config) les utilisateurs et les hashes des mots de passe correspondants, et qui écrase les hashes des utilisateurs administrateurs avec ces derniers :

AAD3B435B51404EEAAD3B435B51404EE (2 hashes LM vides)
et 31D6CFE0D16AE931B73C59D7E0C089C0 (1 hash NTLM vide)
C'EST FAIT ! Lors du prochain redémarrage du système, le compte utilisateur dont on a écrasé les hashes ne demandera plus le mot de passe.

En réalité, ces deux live CD free contiennent bien d'autres outils : par exemple pour enregistrer les hashes extraits sur une clé USB afin de les emmener chez soi et travailler dessus.

:: Cracker le mot de passe

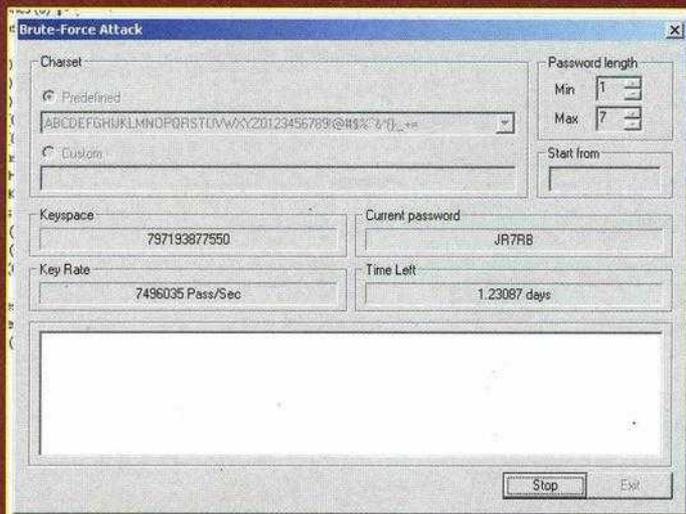
Mais bien sûr, nous ne pouvons pas nous contenter de savoir écraser un mot de passe, pas vrai ? Nous ce qui nous intéresse, c'est de voir si nous sommes vraiment capables de le trouver. Comment faire pour récupérer les hashes

et procéder en toute quiétude ?
Là aussi, il existe 2 solutions :
Si vous avez accès au système cible avec un compte administrateur, vous pouvez par exemple exécuter Cain ou Ophcrack ou encore SamInside (il existe des dizaines de programmes spécialisés dans ce domaine), enregistrer les hashes qui vous intéressent dans un fichier txt et y travailler chez vous à votre aise.
Si vous n'y avez pas accès avec un compte administrateur, vous pouvez par exemple utiliser l'un des 2 CD live cités ci-dessus.

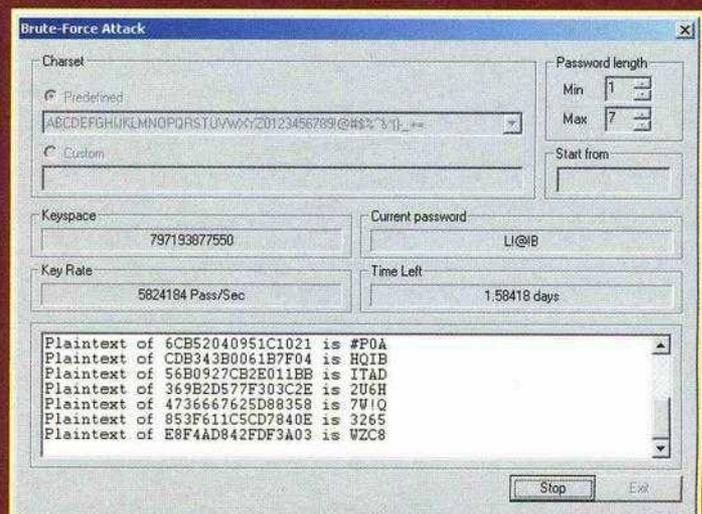
Une fois les hashes récupérés et emportés chez vous, vous pouvez commencer à travailler dessus.

Pour cela, il existe 3 grandes méthodes d'attaque :

- Cette bonne chère vieille attaque par dictionnaire, qui suppose que vous ayez un fichier texte assez gros, comprenant un bel éventail de mots et de dates habituellement utilisés comme mot de passe. La probabilité moyenne pour que ce genre d'attaque fonctionne n'est pas très élevée (autour de 45 %), et dépend de votre dictionnaire et de l'origine du mot de passe (si votre père a verrouillé le PC non pas avec votre nom mais avec le mot de passe qu'il utilise dans son entreprise, alors il est fort probable que le mot de passe soit assez complexe).
- Puis, l'attaque par 'force brute' : le programme calcule les hashes de toutes les combinaisons de caractères possibles et les compare avec les hashes donnés.



⚠ **Une attaque par force brute avec symboles sur un compte, 7,5 millions de tentatives par seconde, 1 à 2 jours de prévu.**



⚠ **Une attaque par force brute avec des symboles sur 28 comptes simultanément, 5,8 millions de tentatives par seconde, 1 à 6 jours**



- Et enfin l'attaque par Rainbow Tables : des tables d'éventuels hashes précompilées que le programme charge en mémoire et compare avec les hashes donnés jusqu'à ce qu'il trouve le bon.

Pour effectuer les tests, j'ai créé sur mon PC des comptes de test. J'ai choisi la longueur des mots de passe (4, 7, 10, 14) et pour chaque longueur, j'ai créé 7 comptes (numérique, alphabet, alphanumérique, alphanumérique+symboles, mélange alphabet, mélange alphanumérique, mélange alphanumérique+symboles, mélange signifiant majuscules et minuscules) avec des mots de passe aléatoires (<http://www.techzoom.net/security-password.asp>). J'ai donc créé au total 28 comptes.

Si vous lanciez une attaque par dictionnaire, je crois bien que vous ne trouveriez rien... il est vrai que certains programmes peuvent même effectuer les remplacements l33t des mots dans le dictionnaire, mais je doute que dans votre txt, il y ait les mots 'rGJitRF' ou 'cwuXNqz' ... :D

Si en revanche, vous tentiez une attaque par force brute, il vous serait alors possible de casser tout type de mot de passe contenant des lettres, nombres et symboles les plus courants et ce, en quelques jours.

Par exemple, avec mon Athlon 64 3800+ @ default 2,4GHz (qui n'est donc pas un foudre de guerre), Cain parvient à effectuer en moyenne plus de 7 millions de tentatives par seconde, avec une prévision d'un jour et demi environ. Si je fais en sorte que Cain attaque les hashes de 28 comptes simultanément, la vitesse chute d'autant plus... Ces délais seraient plus que tolérables, s'il n'y avait pas la troisième option, qui promet d'être beaucoup plus rapide (avec toutefois certaines limites).

:: Et nous en arrivons à l'attaque par Rainbow Tables

En réalité, il n'existe aucune différence entre une attaque par Rainbow Tables, et une attaque par force brute, si ce n'est le fait qu'ici, les hashes de toutes les combinaisons possibles ont déjà été calculés et enregistrés, et que le programme de crack se

contente de charger en mémoire les tables et d'effectuer la comparaison. Ce qui est bien plus rapide que de calculer toutes les combinaisons !!! En attendant, il faut dire que les Rainbow Tables ne sont pas très flexibles.

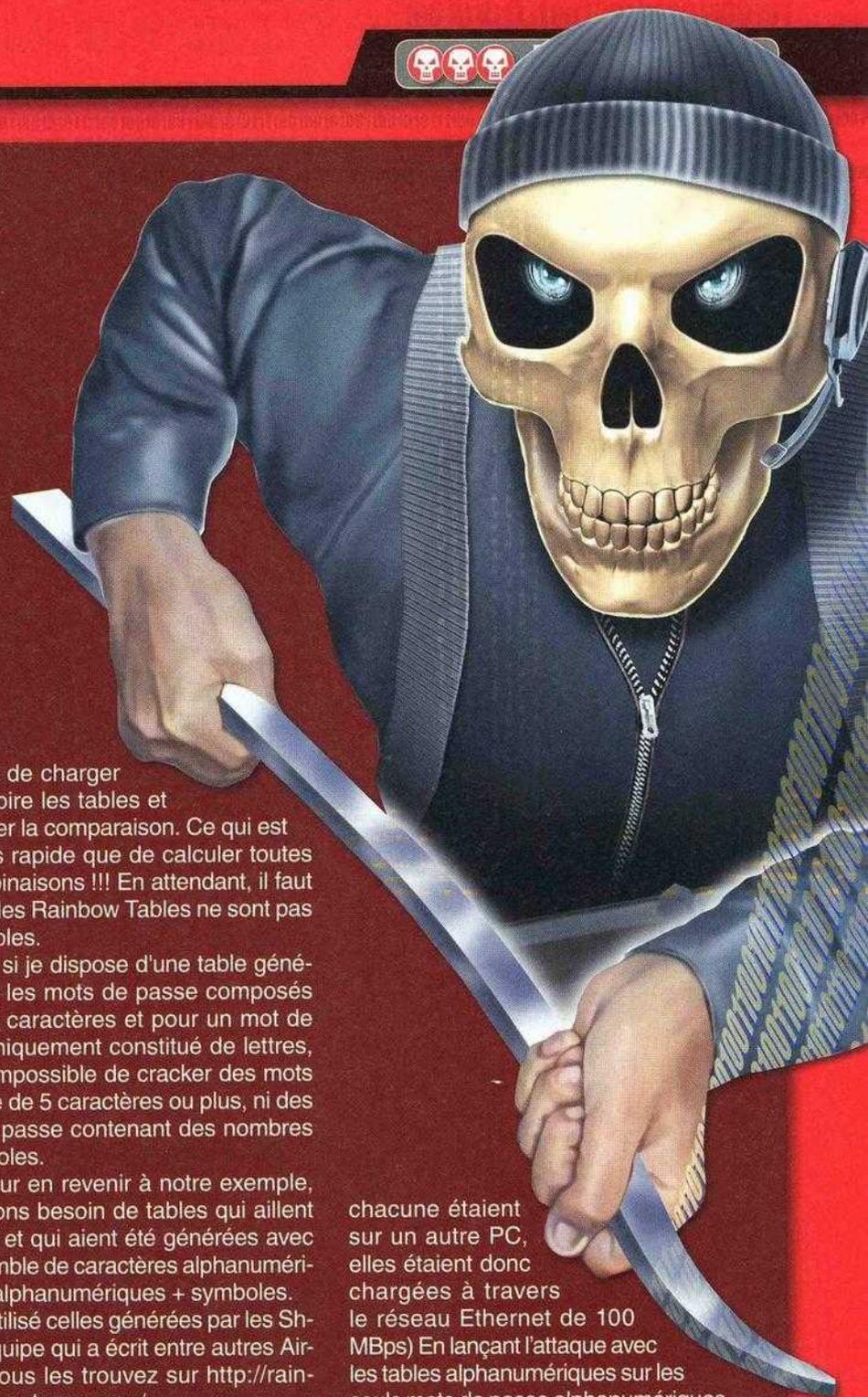
En effet, si je dispose d'une table générée pour les mots de passe composés de 1 à 4 caractères et pour un mot de passe uniquement constitué de lettres, il m'est impossible de cracker des mots de passe de 5 caractères ou plus, ni des mots de passe contenant des nombres ou symboles.

Donc pour en revenir à notre exemple, nous avons besoin de tables qui aillent de 1 à 7 et qui aient été générées avec un ensemble de caractères alphanumériques et alphanumériques + symboles.

Moi j'ai utilisé celles générées par les Shmoo, l'équipe qui a écrit entre autres AirSnort. Vous les trouvez sur <http://rainbowtables.shmoo.com/>

Elles sont assez lourdes : les alphanumériques font 1,22 Go compressées, tandis que les alphanumériques + symboles et espace font 34,4 Go compressées !

Les résultats sont alarmants : en attaquant les 28 mots de passe de test simultanément avec les tables de 34 Go, Cain a mis 14 131 secondes au total (soit un peu moins de 4 heures) dont 4 305 s (presque une heure et quart) uniquement pour charger en mémoire les tables (j'ai 2 Go de Ram, mais les tables d'1 Go



chacune étaient sur un autre PC, elles étaient donc chargées à travers le réseau Ethernet de 100 MBps) En lançant l'attaque avec les tables alphanumériques sur les seuls mots de passe alphanumériques, les délais se réduisent à 12 minutes, dont plus de 7 pour le chargement.

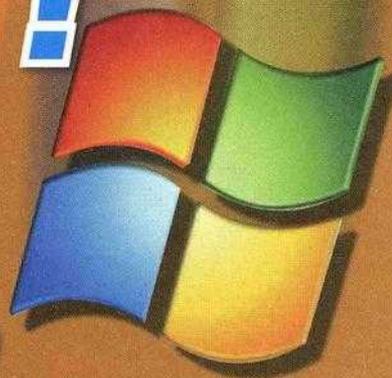
:: Conclusion

Le résultat est sans appel. Si vous voulez que vos mots de passe de XP résistent plus d'un quart d'heure, insérez-y des symboles, ou faites en sorte qu'ils dépassent 14 caractères !

SFlamer

REACTOS, fenêtres libres !

Voici une alternative efficace à Windows pour vous libérer de vos chaînes, sans pour autant renoncer à vos programmes habituels



:: Billet d'humeur

Sympa Windows, non ? Avec cette interface graphique, tous ces programmes, drivers et fonctions. Windows est compatible avec une infinité de programmes, sans parler des nombreux jeux ! Avec lui, tous vos périphériques fonctionneront sans l'ombre d'un problème. Une pure merveille, rien à redire !

Ok, Ok, c'était une blague. En fait, on n'est pas très copains avec Windows. Pas copain du tout, même ! Pourtant, on est parfois bien obligé de l'utiliser. De temps à autre, on a besoin de ce programme spécifique pour pouvoir ouvrir tel ou tel vieux document, on encore lancer ce jeu qui nous plaisait tant dans notre enfance... Vous êtes de vrais hackers ? Alors vous aimez certainement les programmes libres ! Le problème, c'est que vous avez aussi besoin d'un environnement Windows. La solution ? ReactOS bien sûr !!

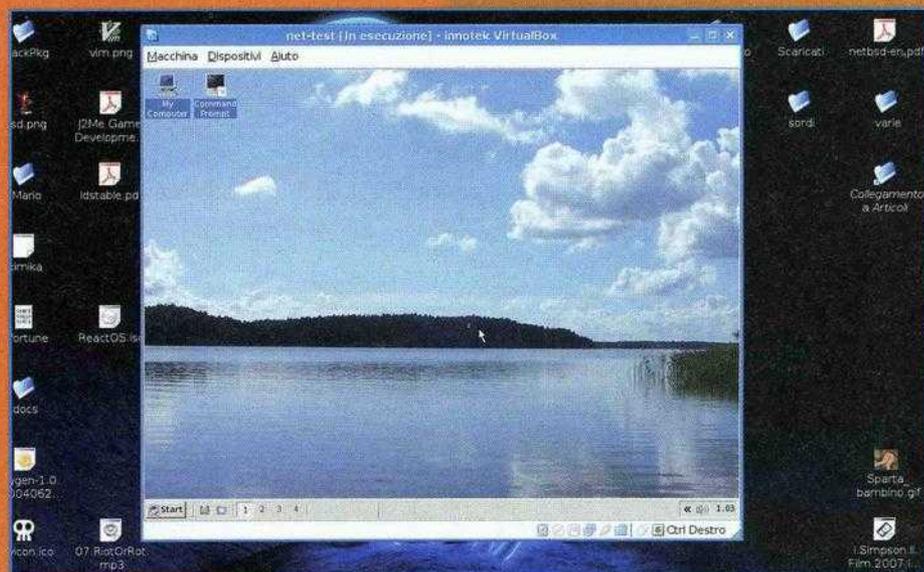
:: C'est quoi au juste ?

ReactOS est un système d'exploitation 100 % Open Source, écrit en

s'inspirant largement de Microsoft Windows.

Sa structure et ses fonctions calquent fidèlement celles proposées par Windows. L'objectif principal étant de fournir un environnement compatible avec Windows XP au niveau des interfaces de programmation. Comme tout programme libre, ReactOS est lui aussi un projet commu-

nautaire, ouvert à toute contribution. La page d'accueil du site propose au téléchargement la toute dernière version du système d'exploitation (la 0.3.3, à l'heure où nous écrivons) avec le CD d'installation et le CD live, et même le code source, sans oublier des machines virtuelles prêtes à l'emploi pour ceux qui ne veulent pas tester ce système en gaspillant un CD :-)



▲ Premier lancement de React OS

te (façon de dire), redémarrage, suivi de quelques petits paramétrages secondaires (type zone horaire ou layout du clavier), mot de passe de l'utilisateur administrateur, nom de l'ordinateur et ainsi de suite. Dernier redémarrage, et votre système sera fin prêt ! Du moins jusqu'au prochain redémarrage :-)

:: Alpha

Vous pensez déjà l'utiliser sur vos PC en remplacement de Windows ? Libre à vous de le faire (c'est votre ordinateur, après tout !), même si l'équipe de développement le déconseille vivement. Car si ReactOS peut faire tourner différentes applications (Opera, OpenOffice 1, Firefox, Quake, Halo, Office, Thunderbird ont déjà été testés, et bien d'autres encore), le système est délivré en version Alpha. Qu'est-ce que ça veut dire ? Qu'il est encore en pleine phase de développement, et qu'il connaît donc encore quelques problèmes de stabilité, même s'il "tourne" correctement. Ainsi, le support de nombreux éléments reste absent, comme les sempiternels périphériques USB. En fouillant un peu dans le système, il n'est pas rare de tomber sur des fenêtres de dialogue vides qui attendent d'être remplies. Cela devrait vous faire réfléchir, sachant que la version Bêta (qui en théorie devrait être plus stable) devrait sortir cette année.

:: Où ça ?

Vous pouvez trouver ReactOS sur <http://www.reactos.org/fr/index.html>. Le site héberge aussi un forum très actif, subdivisé par thèmes, où développeurs et utilisateurs peuvent faire part de leurs doutes. Les principales catégories concernent l'utilisation et le développement, les notes publiques attribuées et les langues spécifiques. Vous y trouverez donc des rubriques entièrement en français. Le site héberge un wiki très sympa, plein de documents sur la structure du système d'exploitation et sur son utilisation, des trucs et astuces, et bien d'autres choses encore

:: Conclusions

ReactOS est un produit vraiment

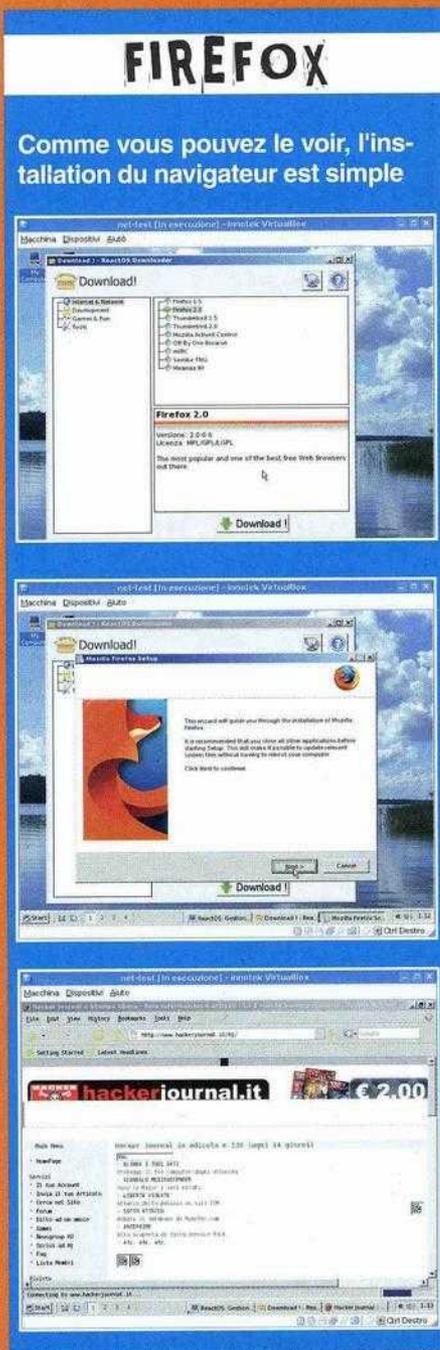
nouveau. Conceptuellement parlant, il est plus innovant que GNU/Linux : s'il atteint ses objectifs, il permettra aux entreprises et à la quasi-totalité des utilisateurs de software propriétaire Windows, de passer à des programmes libres, sans avoir à changer de plate-forme, en conservant donc les anciens programmes. Un projet à suivre et à surveiller !

Lord Belthazor "Sid" Vicious



:: Téléchargement et installation

Vous pouvez le télécharger sur <http://www.reactos.org/fr/download.html>. Choisissez la rubrique "CD d'installation", qui vous mènera sur le site de SourceForge, à la page de téléchargement. Le téléchargement automatique s'effectuera quelques secondes plus tard. Et là, première surprise : le CD d'installation fait à peine 24 Mo ! Vous avez à présent deux possibilités : soit l'insérer dans une machine virtuelle, soit sacrifier un CD. Vous devrez dans tous les cas redémarrer la machine (qu'elle soit réelle ou virtuelle) sur laquelle vous avez installé le CD. Autre surprise : le processus d'installation est identique à celui des systèmes Windows, à une différence près : il est encore plus simple et beaucoup plus rapide ! La procédure d'installation se compose de quelques étapes simples mais néanmoins fondamentales : sélection des disques, paramétrage de leur géométrie (la plupart du temps, le paramétrage par défaut convient parfaitement), création et formatage des partitions, copie des fichiers, installation des boot loader et, comme tout système Windows qui se respec-





Aucune TRACE, pas de VISAGE

Le moindre pas sur Internet et vous voilà tracé ! Mais si vous ne souhaitez pas laisser d'empreintes sur votre passage, voici comment procéder...

:: Les bases

L'objectif de cet article ? Vous donner des bases en matière d'anonymat. Sur la question : peu d'outils (mis à part les "anciens" tels que GPG, présenté plus loin), mais beaucoup de concepts. Pourquoi ? Pour l'heure, les outils existent, certes, mais rien n'est moins sûr quant à leur avenir. Les concepts eux, sont toujours valables. Partons du principe légitime que vous n'avez rien à cacher (nous ne sommes pas des lamers), mais que vous souhaitez protéger votre vie privée et vous instruire en la matière. Bien sûr, cet article n'est en aucun cas une encyclopédie sur les outils d'anonymat. Nous vous présenterons ici les outils les plus connus et les plus utiles, ainsi qu'une

brève ébauche de leurs fonctionnalités, sans oublier les concepts les plus intéressants. Les lecteurs les plus agueris pourront approfondir eux-mêmes la question, à travers les liens suggérés (mais n'oubliez jamais que votre meilleur ami reste Google !).

SERVICES

:: A la source

Si vous êtes connecté à Internet, alors vous êtes déjà identifié. Pourquoi ? Les fournisseurs d'accès ont listé des accès au Grand Réseau. Et c'est justement grâce à ces listages que la police parvient à déjouer des

escroqueries basées sur le phishing, et à arrêter de jeunes lamers qui tentent de percer des serveurs à travers le réseau, après avoir lu les volumes de l'encyclopédie de Lord Shiva. Si vous souhaitez réellement surfer en tout anonymat, vous devez agir à la source, en vous abonnant sous un faux nom (il n'est pas difficile de s'en procurer un avec les providers qui fournissent un accès sur des lignes analogiques ou lignes ISDN), ou encore en vous connectant à l'œil sur les réseaux wireless d'autrui... Bien sûr, être anonyme est une chose, le rester est plus difficile. Voici quelques bonnes combines pour garder l'anonymat : changer d'adresses e-mail, de points de connexion (par exemple, ne pas toujours se

connecter depuis le même réseau wireless), d'identités virtuelles, etc.. Pourquoi est-il aussi difficile de garder l'anonymat ? Réfléchissons un peu. Si c'était si facile, ne serions-nous pas déjà tous anonymes ?

:: Serveur mandataire (proxy)

Autre solution pour garder l'anonymat, plus simple et moins extrême (et donc moins efficace) : les proxies.

Que font les proxies ? Ils s'interposent tout simplement entre le client et le serveur, en servant de médiateur pour la communication. Exemple : un hacker français (voyez-vous ça!), un host brésilien, un proxy russe. Au début, la connexion s'établit ainsi :

hacker (France) -> host (Brésil)

Le hacker paramètre son ordinateur pour faire passer les communications à travers le proxy russe. A présent, les paquets effectuent ce parcours :

hacker (France) -> proxy (Russie) -> host (Brésil)

Le client se connecte au proxy, fournit l'adresse du serveur auquel se connecter, ainsi que l'adresse de la ressource à laquelle il souhaite accéder, puis il se met en attente. Le proxy se connecte à l'adresse du serveur fournie, prend la ressource, et la renvoie au client. Le client reçoit la ressource.

Toutefois, le serveur ne logue (en jargon, cela signifie "enregistre") que l'adresse du host qui a effectivement effectué la connexion et la demande, à savoir le proxy. Le proxy est donc beaucoup plus pratique que les autres méthodes précédemment présentées. Mais les lecteurs les plus aguerris se poseront sûrement une question : "pourquoi ces proxies sont-ils donc moins efficaces ?" Tout simplement

parce que généralement, nous ne sommes pas les administrateurs des proxies, et neuf fois sur dix, nous ne pouvons pas savoir si le proxy est effectivement libre et s'il "rend anonyme", ou si les administrateurs ont paramétré l'enregistrement des demandes, des IP, et des hosts contactés, avec la date et l'heure.

S'il en était ainsi, et après avoir retrouvé le proxy, la police pourrait les obliger à fournir les enregistrements des demandes, et remonter ainsi à la source des requêtes (à savoir le hacker).

:: Tor

Tor est une solution relativement récente, totalement dans l'esprit du web 2.0.

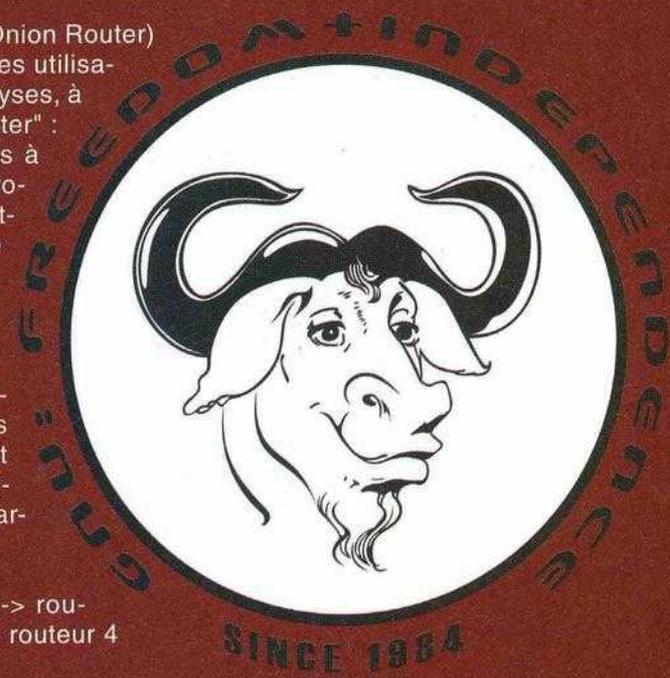
Le réseau Tor (The Onion Router) protège le trafic de ses utilisateurs contre des analyses, à travers les "onion router" : des machines mises à disposition par des volontaires, qui permettent le trafic anonyme en sortie et la réalisation de services anonymes cachés. De quelle façon ? Si dans l'exemple précédent, les paquets effectuaient le trajet hacker-host, ils effectuent désormais le parcours suivant :

hacker -> routeur 1 -> routeur 2 -> routeur 3 -> routeur 4 -> routeur 5 -> host

Un trajet franchement plus long, mais qui n'est pas le réel point fort de Tor. L'avantage avec Tor, c'est qu'une fois qu'un hacker a envoyé une demande au routeur 1, celui-ci choisit au hasard quel autre routeur du réseau Tor utiliser. Chaque routeur ne

connaît que le PC qui lui a transmis la demande. Il ignore donc tout du PC qui a lancé la demande, tout comme il lui est impossible de contrôler la connexion. Et (cerise sur le gâteau :P) le trafic entre un routeur et le routeur suivant est crypté par un système d'encryptage à clé publique. Mais Tor ne protège pas seulement la navigation. Il peut également rendre anonyme le trafic TCP normal, à travers le mécanisme décrit ci-dessus. Tor peut donc être aussi utilisé avec des protocoles tels que POP3, SMTP, SSH... Tout le trafic des paquets TCP peut donc également passer par Tor.

Toutefois, même si le protocole d'"onion routing" utilisé par Tor se caractérise par sa faible latence, les communications via tor sont en géné-



ral lourdement ralenties, à cause du nombre élevé de hosts à travers lesquels les paquets doivent transiter. Sans doute consacrerons-nous un jour un article à Tor, pour découvrir toutes ses spécificités.

En attendant, vous pouvez vous documenter en consultant l'adresse suivante : <http://tor.eff.org/index.html>.





OUTILS

:: Au grand jour

Souvent, pour de multiples raisons, nous ne pouvons ou ne voulons utiliser Tor, ni de proxy ou autres. Nous devons utiliser un canal de communication normal. Bref, un sacré problème ! Que faire dans ce cas ?

Utiliser l'encryptage à clé publique. Contrairement à l'encryptage à clé privée, ou One Time Pad, ce type d'encryptage se base sur deux clés : une pour chiffrer et une autre pour déchiffrer. La spécificité de ces clés ? C'est qu'il est mathématiquement impossible de remonter à une clé grâce à l'autre.

Voici l'outil qui vous permettra d'utiliser ce type d'encryptage : GnuPG (GNU Privacy Guard). Les développeurs le présentent ainsi : "GnuPG permet de chiffrer et de signer numériquement ses données et

communications. Il propose un système de gestion des clés polyvalent et des modules pour accéder à tout type de liste de clés publiques. GnuPG, connu également sous le nom de GPG, est un outil en ligne de commande qui s'intègre facilement aux autres applications, grâce à la disponibilité de nombreux front end et de bibliothèques"

Bref, quelle puissance ! Disponible pour GNU/Linux, Windows, Mac, et différentes formes de BSD, cet outil vous permettra d'empêcher toute violation de vos données, du moins s'il est bien utilisé.

Pour approfondir le sujet, vous pouvez commencer par : [www.gnupg.org/\(fr\)/index.html](http://www.gnupg.org/(fr)/index.html), et trouver de la documentation à l'adresse suivante : [www.gnupg.org/\(fr\)/documentation/guides.html](http://www.gnupg.org/(fr)/documentation/guides.html).

De par sa nature, GnuPG fonctionne parfaitement bien sur des systèmes style UNIX, ayant justement été développé sur ces systèmes. Mais il est également disponible pour Windows, avec des interfaces graphiques appropriées.

:: Hardcore

Nous en arrivons aux choses sérieuses : services de messagerie anonymes et fichiers système cryptés.

Sans doute aurez-vous l'impression que certaines des choses que nous dirons contredisent ce que nous avons écrit dans certains numéros précédents de HNM. Mais pas de panique ! Nous vous montrons tout simplement de nouveaux services.

:: Fichiers système cryptés

Bon nombre d'entre vous ont déjà sans doute pris l'habitude de crypter leurs fichiers avant de les faire circuler sur le Net. Un système qui vous protège certes des interceptions.

Mais comment faire pour vous défendre face à une attaque physique lancée contre votre machine ? En outre, si quelqu'un vous vole votre ordinateur portable, que faire pour éviter qu'il puisse accéder à toutes vos informations ? La solution consiste à tout crypter : toute la partition. Comment ? Tout dépend du *type* de système d'exploitation. Tous les bons systèmes (style GNU/Linux et tous les *BSD) disposent d'un moyen interne et largement opérationnel pour le cryptage. OpenBSD l'emporte largement dans ce domaine : une fois installé, tout est déjà prêt pour paramétrer des fichiers système chiffrés.

Pour GNU/Linux, vous devrez appliquer certains patches au kernel, ou activer les options de chiffrement

Tor: Un système de connexion anonyme à Internet

Tor est un projet logiciel qui aide à la défense contre l'analyse de trafic, une forme de surveillance de réseau qui menace les libertés individuelles et l'intimité, les activités commerciales et relationnelles, et la sécurité d'état. Tor vous protège en faisant rebondir vos communications à l'intérieur d'un réseau distribué de relais maintenus par des volontaires partout dans le monde : il empêche qu'une tierce personne scrutant votre connexion internet connaisse les sites que vous avez visité, et empêche les sites que vous avez visité de connaître votre position géographique. Tor fonctionne avec beaucoup de nos applications existantes, comme les navigateurs web, les clients de messagerie instantanée, les connexions à distance et tout un nombre d'application se basant sur le protocole TCP.

Des centaines de milliers de gens à travers le monde utilisent Tor pour une grande variété de raisons : les journalistes et les blogueurs, les défenseurs des Droits de l'Homme, les agents d'application des lois, les soldats, les entreprises, les citoyens de gouvernement répressif, et juste des citoyens. Regardez [Qui Utilise Tor ?](#) sur cette page pour des exemples typiques d'utilisateurs Tor. Voyez la [page d'ensemble](#) pour une explication plus détaillée de ce que Tor fait, pourquoi cette diversité d'utilisateur est importante et comment Tor fonctionne.

Il y a trois choses fondamentales à connaître avant de commencer.

1. Tor ne vous protège pas si vous ne l'utilisez pas correctement. Voyez notre [liste d'avertissements](#) et assurez vous de suivre avec attention les [instructions pour votre plateforme](#).
2. Même si vous configurez et utilisez Tor correctement, il y a encore [des attaques potentielles qui peuvent compromettre la capacité de Tor à vous protéger](#).
3. Aucun système anonyme n'est parfait à ce jour, et Tor ne fait pas exception : vous ne devriez pas vous fier intégralement au réseau Tor si vous avez besoin d'une protection anonyme totale.

La sécurité de Tor s'accroît autant que le nombre d'utilisateur augmente et tant que le nombre de volontaire pour [monter un relay](#) croît. (Ce n'est pas aussi compliqué que ce que vous pensez, et ça peut significativement [étendre votre propre sécurité contre quelques attaques](#).) Si faire tourner un relais n'est pas pour vous, nous avons besoin d' [aide sur plusieurs points du projet](#), et nous avons besoin d'un financement pour [continuer à rendre le réseau Tor plus rapide et plus facile à utiliser tout en maintenant une bonne sécurité](#). N'hésitez pas à [contribuer financièrement](#).

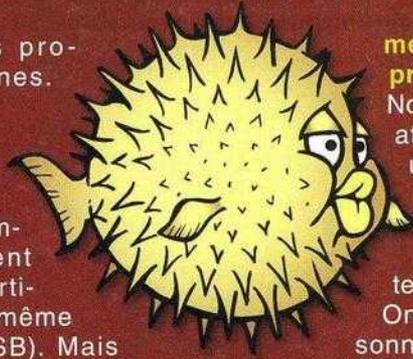
Nouvelles

- Fév 2008: Le [Conseil d'Administration](#) accueille [Isaac Mac](#) au Conseil. Nous remercions Rebecca McKinnon pour son soutien et ses contributions au projet.
- Fév 2008: Tor est heureux de vous annoncer l'ouverture du [blog Tor officiel](#).
- Jan 2008: [Tor 0.1.2.19](#) (la dernière version stable) corrige une grosse fuite mémoire sur les relais de sortie, rend les règles de sortie

dans la configuration du kernel, puis passer à la configuration à proprement dit des périphériques virtuels cryptés. Toujours à la traîne, Windows ne propose pas de système fonctionnel et polyvalent comme celui des autres systèmes cités ci-dessus. Il vous faudra donc

recourir à des programmes externes.

TrueCrypt (www.truecrypt.org/) fournit un moyen simple et polyvalent de créer des partitions cryptées (même sur des clés USB). Mais pour une analyse plus approfondie, nous vous renvoyons à l'article sur cet outil publié dans ce numéro. Pas mal toutes ces méthodes... Et leurs inconvénients ? Il n'en existe qu'un seul : si vous oubliez votre mot de passe, vous n'aurez ***AUCUN*** moyen de récupérer vos données (ce qui est, au final, plutôt logique).



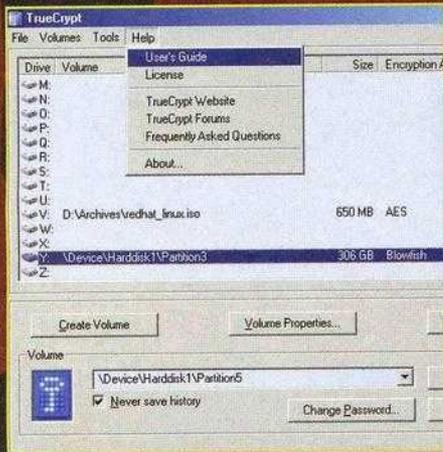
méthodes à utiliser pour protéger votre vie privée.

Nous souhaitons cependant attirer votre attention sur un problème purement italien : l'Italie est devenue le pays comptant le plus grand nombre d'interceptions annuelles.

On estime ainsi que 3 personnes sur quatre ont eu au moins un appel téléphonique intercepté. Les temps sont durs pour préserver notre vie privée ! C'est pourquoi nous vous conseillons vivement de vous doter (et bien sûr de l'utiliser) d'un outil de cryptage lourd, tel que GnuPG. Et nous vous conseillons également de vous doter d'un système d'exploitation transparent, comme GNU/Linux. Vous aurez ainsi connaissance des activités lancées sur votre ordinateur.

Avec Windows, vous ne pourrez que l'imaginer, sans aucune sécurité.

Emanuele Santoro



:: Conclusion

Après avoir lu cet article, vous devriez en savoir un peu plus sur les

PROXY

Voici la liste non exhaustive de quelques-uns des proxies opérationnels en ce moment :

| | | | | | |
|-------------|---------------|---------------|---------------|---------------|---------------|
| 3proxy.org | concealme.com | freeproxy.ca | hujiko.com | netsack.net | proxify.com |
| 75i.net | cpr0x.com | fsurf.com | idoxy.com | pimps.com | proxyguy.com |
| anypost.com | cyberbite.com | gouc.fr | ipzap.com | phproxy.org | proxypip.org |
| arnit.net | dzzt.com | hideip.be | liteproxy.com | poxys.us.to | proxylord.com |
| bypassit.be | fireprox.com | httpproxy.com | mrproxy.com | proxifree.com | proxyspy.com |

Année 5 – n° 22 Bimestriel
février - mars 2008

Hacker News Magazine
Et son complice italien
Hacker Journal

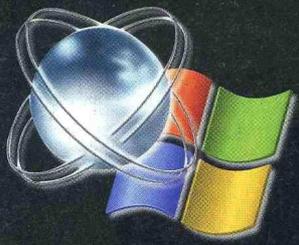
1ers magazines européens Hacker
Boss: TheGuilty@hackerjournal.it
Les camarades de la rédaction européenne :
 Gregory, Fred, Damien Bancal,
 One4Bus, Max, G. Tronconi,
 K2der, Sylvain, Silvio De Pecher,
 Contents by MDR.

Traduction et adaptation :
 Laurent et Sylvie Arsena

Mise en page : Selestudio
Couverture: Daniele Festa
Editeur :
 WLF Publishing SRL
 Via Donatello 71
 00196 Roma
Imprimeur : Roto 2000,
 Via Leonardo da Vinci 18/20
 Casarile (MI) Italy
Distribution:
 MLP - 55 bd de la Noirée
 ZA de Chesnes, 38070 St Quentin Fallavier

Directeur de la publication :

Teresa Carsaniga
Dépôt légal : à parution
ISSN : en cours
Copyright WLF Publishing
 Les droits sont réservés et protégés
 Pour la version imprimée.
 La rédaction n'est pas responsable des
 textes, documents, photos, dessins qui lui
 sont communiqués et n'engagent que la
 responsabilité de leurs auteurs.
 Sauf accord particulier et publiés ou non, ils
 ne sont pas renvoyés.
 Les indications de prix et d'adresses
 sont de l'information fournie sans
 aucun but publicitaire.



REACTOS : L'ALTERNATIVE GRATUITE À WINDOWS

MODCHIP CONSOLES

comment modifier sa

 **PLAYSTATION**

 **Wii**

 **XBOX360**



WLF
PUBLISHING

N° 22 / février / Mars 2008 - BEL/LUX : 2,40 € SUISSE : 4 FS
DOM : 2,50 € - TOM : 4,90 XPF - MAROC : 25 MAD

L'UNIVERS VIRTUEL sous l'attaque des **PIRATES**

WORLD OF WARCRAFT