

TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

2.00 €
0% DE PUBLICITE
JUSTE DES ARTICLES

HACKER news Magazine

LE MAGAZINE 100% SECURITE PLUS LU



L'ARMÉE
SE PRÉPARE À UNE
CYBERGUERRE!

PIRATE BAY

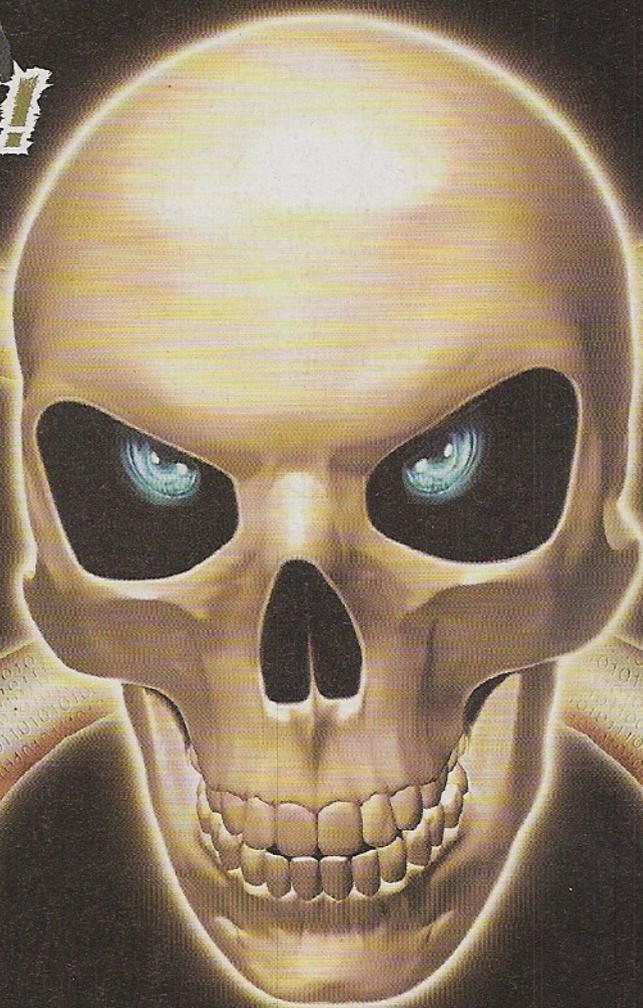
les Blogs enfin
100% LIBRES



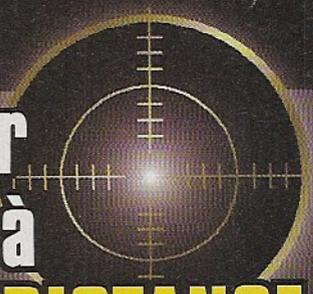
WAREZ:
RAZZIA DE LA **POLICE!**

BOTNET
Bientôt tous des zombies ?

TÉLÉPHONE
Lire les sms, écouter les appels
d'un téléphone portable c'est possible !



Toutes les **TECHNIQUES** pour
ESPIONNER à **DISTANCE**



Année 5 – n° 24 Bimestriel
Août - Sept 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, Ferluc, Damien Bancal,
One4Bus, Max, G. Tronconi,
K2der, Sylvain, Silvio De Pecher.

Traduction et adaptation :
Laurent et Sylvie Arsena

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:
NMPP

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.

Lamer ('lae'mr)

Aspirant cracker, aux capacités et connaissances informatiques limitées,
souvent maladroit et disposé à mener des actions douteuses et nuisibles.

Editorial

HACKER
Magazine

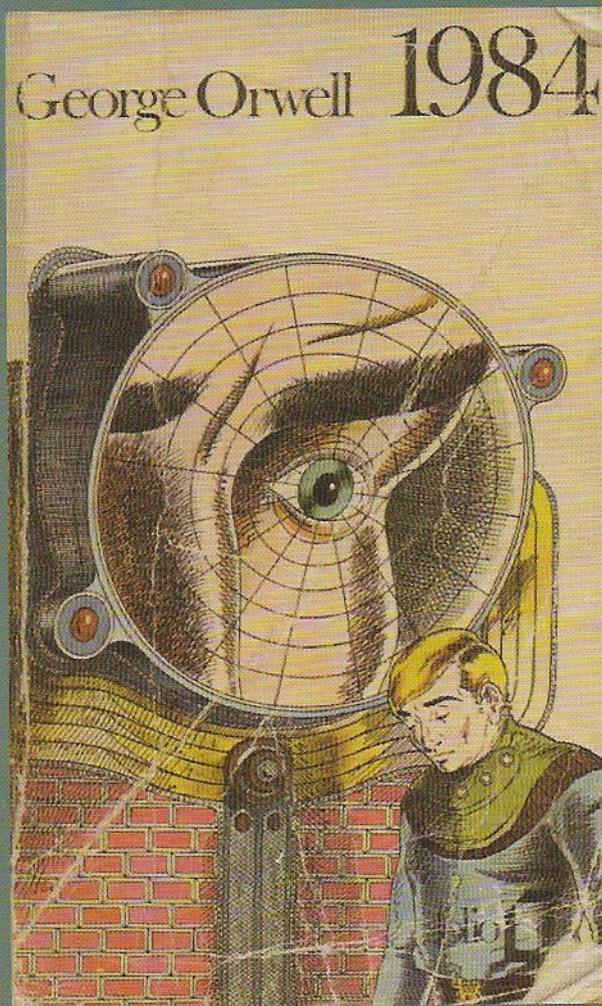
Big Brother vous regarde... et en plus vous le savez !

En allant me promener sur un marché aux puces, j'ai eu la chance de tomber sur un livre édité en France, en 1977. Un bouquin écrit en 1950, voilà plus de 58 ans, une éternité pour nous qui n'étions même pas nés. En glissant mes yeux sur la couverture, je suis tombé sur ce petit texte « De tous les carrefours importants, le visage à la moustache noire vous fixait du regard. Il y en avait un sur le mur d'en face. BIG BROTHER VOUS REGARDE, répétait la légende, tandis que le regard des yeux noirs pénétrait les yeux de Winston... Au loin, un hélicoptère glissa entre les toits, plana un moment, telle une mouche bleue, puis repartit comme une flèche, dans un vol courbe. C'était une patrouille qui venait mettre le nez aux fenêtres des gens. Mais les patrouilles n'avaient pas d'importance. Seule comptait la Police de la Pensée. »

En relisant la 4ème de couverture du roman « 1984 » de George Orwell, on peut se demander comment réagirait cet écrivain de génie si nous lui expliquions nos vies d'aujourd'hui. Internet, les cartes à puces, la cyber surveillance, les lois ayant pour mission de nous protéger et se transformant de plus en plus en ce Grand Frère dépeint par Orwell. Pas de doute, il nous regarderait avec de grands yeux ouverts et se moquerait de nous à gorge déployée.

Pourtant, aujourd'hui, force est de constater que sa peinture d'un terrifiant monde totalitaire n'est plus qu'une virgule dans un jeu vidéo dont nous sommes tous devenus les héros ! Le plus inquiétant est que nos législateurs, qui votent à tour de bras des lois « Internet », ... n'ont pas un wagon de retard, mais des trains de retard. Un seul exemple. La surveillance des internautes utilisateurs de système de P2P. Depuis bien longtemps les pirates, les vrais, ont trouvé de nouvelles méthodes pour diffuser leurs copies. Et la riposte graduée, que souhaite mettre en place en France, n'est pas du tout prévue face à ces nouveaux modes de diffusion. Dans dix ans elle le sera peut-être !

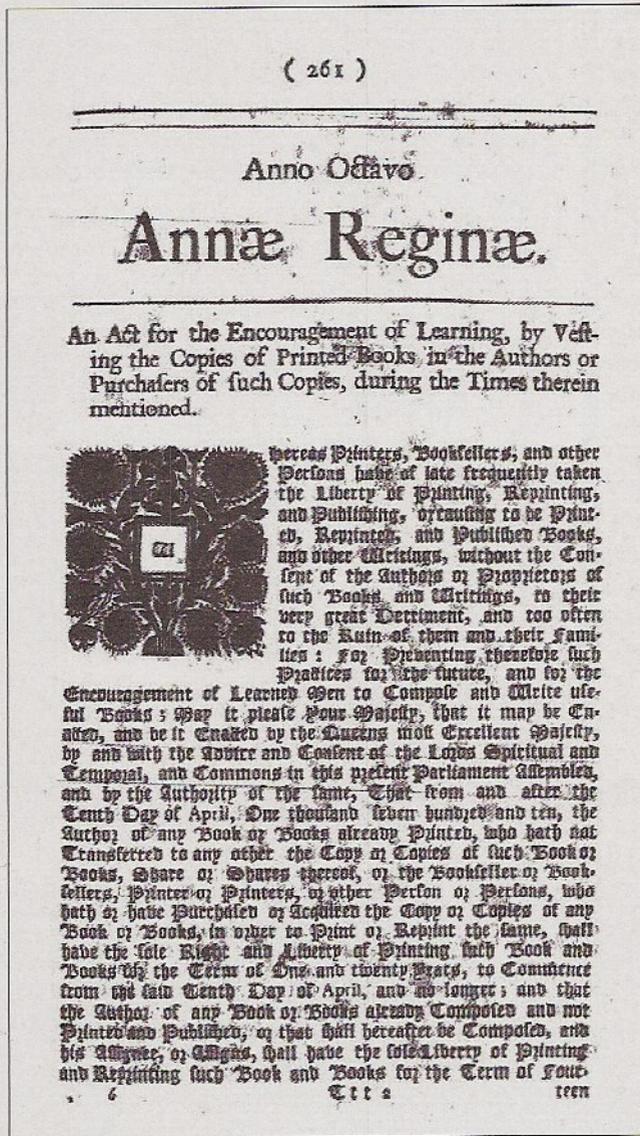
Espérons quand même que dans dix ans, la patrouille « qui venait mettre le nez aux fenêtres des gens » ne soit toujours qu'un roman.



ILS EN VEULENT TOUJOURS PLUS !

Depuis l'an dernier, les groupes de pression de l'industrie artistique ont engagé une opération de grande envergure pour obtenir l'extension de la durée de protection des droits des interprètes. Tout a commencé quand l'AEPO-ARTIS, la fédération européenne des syndicats d'artistes-interprètes, a publié dans son rapport 2007 les lignes suivantes : « Au moment où un grand nombre d'enregistrements sonores et audiovisuels européens de haute qualité, qui sont populaires et font encore l'objet d'exploitations, parviennent à la fin de la période de protection, il semble justifié d'étendre la durée de protection des droits des artistes interprètes à 95 ans. » Comprenez, 95 ans après l'enregistrement ou 95 ans après la performance. Par ce texte, l'organisation se contentait d'aligner ses revendications sur la durée de protection acquise par les artistes états-uniens en 1988, lors de l'adoption du Sonny Bono Copyright Term Extension Act (*). Bref, une « rente à vie », voire un peu plus, comme le dénonce avec fermeté et régularité Guillaume Champeau sur le site numerama.com.

Or ces revendications ont été entendues dès février 2008 par le Commissaire européen au marché intérieur et aux services, Charlie Mc Creevy qui les a ensuite reprises lors du discours qu'il a prononcé fin avril dans le cadre de la Journée mondiale de la Propriété intellectuelle.



que le choix d'allonger la période de protection des œuvres est une mesure discutable. Condamnable même si l'on considère que, depuis le « Statute of Anne » de 1710, première délibération sur la protection du droit d'auteur (droit de « reproduction » serait plus juste), il est entendu que cette protection ne saurait pas entraver la création artistique. Mc Creevy lui-même rappelle que : « les droits accordés aux artistes interprètes doivent accompagner le développement d'un marché culturel fort et dynamique et contribuer à son enrichissement ».

En fait, il serait bien plus judicieux de répartir plus équitablement les droits considérables que touchent les grosses vedettes du showbiz, afin d'en faire profiter tous ceux qui contribuent à leur succès. Car, en bloquant « ad vitam aeternam », serait-on tenté de dire, ces droits, comment peut-il imaginer, ce bon commissaire bruxellois qu'il va encourager les créatifs à créer ? Rappelons simplement que les auteurs bénéficient d'ores et déjà d'une protection s'étendant aux 70 années suivant leur mort. Ce qui non seulement profite à leurs héritiers - dont il n'est pas particulièrement établi qu'ils aient le même génie créatif qu'eux - et peut leur suffire pour s'endormir sur leur magot dès leur premier succès...

Pour lui, il s'agit de garantir aux interprètes - y compris de studio - un revenu tout au long de leur vie et un droit de contrôle sur leurs performances.

Et pourquoi pas, après tout ? Il ne semble pas absurde de vouloir offrir à tous les artistes une juste rétribution. Sauf

(*) Du nom du Bono de Sonny and Cher

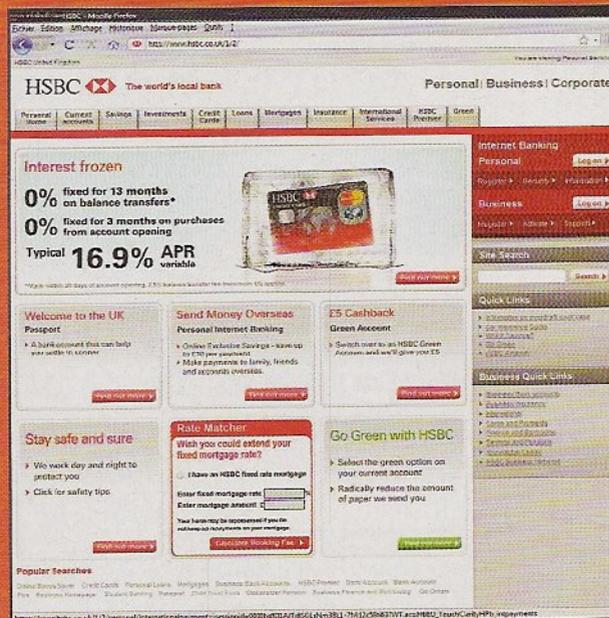


SAUVEGARDE EN FAMILLE

Un tiers de consommateurs basés aux États-Unis et au Royaume-Uni a avoué avoir fait une copie d'un DVD au cours des 6 derniers mois selon un rapport des consultants de Futuresource. Un sondage effectué sur un panel de 3,613 américains et 1,718 britanniques. L'étude tente de démontrer que le «piratage familial» reste une habitude bien ancrée malgré les lois en vigueur interdisant ce genre de pratique. Des copies pour une utilisation personnelle expliquent 32 % des américains et 36 % des anglais sondés. Futuresource note, pourtant, qu'environ 62 % des américains et de 49 % des anglais indiquent faire des copies «légitimes» de leurs nouveaux DVDs qu'ils viennent d'acquérir. La grande majorité des «copieurs» interrogés pensent que la loi est avec eux. Ce qui n'est pourtant pas le cas.

BRAQUAGE NUMÉRIQUE

Jagmeet Channa, 25 ans, était employé par la banque HSBC. Le moins que l'on puisse dire est qu'il a pris son travail à cœur. Il s'est occupé de manière particulière des comptes clients. Il a été condamné à 9 ans de prison pour blanchiment d'argent, et 90 mois ferme pour avoir tenté de voler 141 millions de dollars des comptes en banque ouverts chez son employeur. L'escroc a plaidé coupable le 7 juillet dernier devant un tribunal anglais. Il faut dire aussi qu'en avril dernier, il avait utilisé les codes d'accès de collègues pour faire transiter 30 millions d'euros sur un compte ouvert dans la banque Barclay's et 60 millions d'euros qu'il a tenté de transférer au Maroc. Les policiers de Scotland Yard indiquent que Channa a tenté l'une des plus importantes fraudes électroniques de ces dernières années.



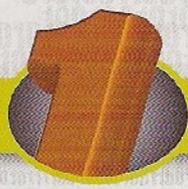
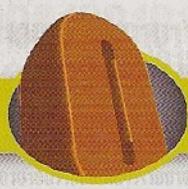
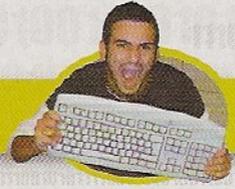
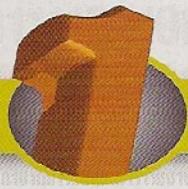
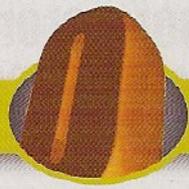
VOL DE DONNÉES SUR DES SITES D'OFFRES D'EMPLOIS

La société PrevX, un chasseur de virus informatiques, a découvert un outil très particulier. Un logiciel en ligne, codé en PHP, permettant à des pirates russes d'intercepter des données privées déposées par des demandeurs d'emplois sur des sites dédiés américains. Mission de ce programme, infiltrer les sites Monster.com,

AOL Jobs, Ajojobs.com, Careerbuilder.com, CareerMag.com, Computerrjobs.com, Hotjobs.com, Jobcontrolcenter.com, Jobvertise.com et Militaryhire.com. Un code capable d'extraire des détails personnels trouvés dans les CVs (noms, adresses de courrier électronique, adresses personnelles et employeurs actuels). Les intrus commercialisent ensuite les contenus ou proposent, par ICQ, aux propriétaires des données de les effacer de leurs bases pirates contre quelques centaines de dollars.

RESPONSABLE MAIS PAS COUPABLE

Une cour de justice de Francfort (Allemagne) a décrété que les utilisateurs Internet ayant eu leur routeur wifi piraté n'étaient pas responsables des actes des pirates ayant utilisé ce passage sans fil. Une décision intéressante car elle fait suite à des téléchargements illicites sur des sites de P2P. Des copies que n'auraient pas effectué les internautes peu regardant du côté



HOT NEWS

LE PIRATAGE À SON PRIX

La cyber-criminalité est une activité fort lucrative, l'éditeur de logiciels de sécurité informatique, G DATA, l'affirme en révélant les prix qu'il a pu constater chez les pirates. A première vue, la cyber-criminalité est une activité fort lucrative ! 2 à 25\$: informations de carte de crédit (le prix est fonction des informations disponibles : code, date d'expiration, nom du propriétaire...); 7\$: compte Paypal; 8\$: compte World of Warcraft; 15\$: infection de 1 000 systèmes; 25 à 50\$: 1 million d'adresses e-mail; 25 à 100\$: par attaque de déni de service (attaque DDoS) avec les 10 premières minutes offertes, puis 20\$ l'heure et 100\$ la journée; 100 à 3 000\$: par exploit; 5 000 à 50 000\$: la faille de sécurité inconnue.

VILAIN PETIT CANARD CHEZ HP

Atul Malhotra, un ancien vice-président de la division Imaging & printing de chez HP, a tout perdu. Son boulot, sa femme et sa liberté. Il a été inculpé, fin juin, pour le vol présumé de secrets commerciaux d'un concurrent de HP. La victime ? Une des sociétés pour qui il avait travaillé, IBM. Il y occupait, avant d'intégrer HP, le poste de directeur des ventes Imprimante. Le Wall Street journal explique qu'en mars 2006, Atul aurait récupéré un document contenant des informations confidentielles relatives à la facturation de clients. Deux mois plus tard, il rejoint HP avec les données et les communiquera à ses nouveaux patrons. Une très mauvaise idée, car IBM a été prévenu. Pas sûr qu'il retrouve un boulot rapidement le Atul !

LES SPORTIFS DE LA POLICE PIRATÉS

Un pirate informatique, un hacktiviste pour la cause palestinienne, est passé par le serveur Internet du site France Police Sport (france-police-sport.org). Ce site référence toutes les activités sportives de la police nationale. Autant dire que le pirate a tapé sur un espace qu'il vaut mieux éviter, surtout si le défacteur réside sur le territoire hexagonal. Connu sous le pseudonyme de \$n!per_pal, un membre du groupe Hell Team, l'intrus a affiché le drapeau Palestinien, quelques noms d'oiseaux et son idée de la politique internationale. Le site a été corrigé quelques minutes après son passage mais le pirate avait eu le temps de référencer son attaque sur le site de Zone H. A première vue un piratage de masse, d'autres sites hébergés sur le même serveur ont subi une modification identique au même moment.

Bonne pioche pour la police belge

Des agents de la Computer Crime Unit de la police fédérale judiciaire de Bruxelles, la CCU, ont stoppé un groupe de pirates sur internet qui proposaient des films illégaux, des séries et des albums, principalement d'auteurs belges. Cette action est la conséquence

d'une plainte de la Belgian Anti-piracy Federation. Il s'agissait de membres de ce qu'on appelle un « release group », des groupes de pirates organisés qui ont pour objectif d'obtenir le plus rapidement possible de nouveaux films, séries, albums musicaux, etc.

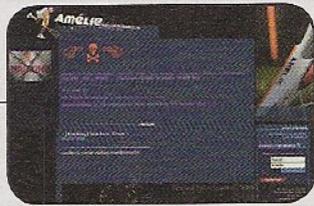
de la sécurité de leurs connexions wifi. Certains petits malins risquent d'ouvrir leur wifi et télécharger tranquillement. Torrentfreak explique que cette même cour d'appel de Francfort a décrété que les parents n'étaient pas responsables des infractions liées aux droits d'auteurs réalisées par leurs enfants.



La police italienne met fin au site DownRevolution.net

La Guardia di Finanza, section de la police italienne, n'a pas peur de s'afficher sur le réseau des réseaux. Elle a fait fermer le site Downrevolution.net et l'a revendiqué sur la page du site délictueux. Une méthode à l'américaine avec un nom très « warez » pour cette action, baptisée : Operazione DownRevolution. DownRevolution diffusait, via des liens renvoyant chez RapidShare, MegaUpload, etc., des films, logiciels et autres mp3 piratés. 4 administrateurs ont été arrêtés, dont trois mineurs. 17 ordinateurs, 3 disques durs, près de 490 DVD et 5.698 œuvres pirates ont été saisis. Un espace qui comptait 30.000 membres et existait sur la toile depuis 2007.





MAURESMO PIRATÉE

Le jour de ses 29 ans, Amélie Mauresmo voit son site Internet piraté. Un cadeau d'anniversaire un peu particulier signé par un pirate informatique connu sous le pseudonyme de Scarface Team. « J'ai voulu alerter la sportive, explique-t-il, mais personne ne m'a répondu ». L'internaute a donc modifié une page en indiquant, entre autres «Le site contient une faille de sécurité importante veuillez la corriger». Dans la même ambiance, mais cette fois par un pirate qui n'avait pas l'intention d'aider, le site du comité d'Ingrid Betancourt a été modifié quelques heures après sa libération. Le barbouilleur a profité d'une faille pour afficher une image.

UNION SECRÈTE CONTRE FAILLE INTERNATIONALE

Une faille qui menaçait la sécurité et l'intégrité du réseau Internet à l'échelle mondiale a été corrigée, au début du mois de juillet, par de grandes entreprises informatiques du monde. Une union sacrée et secrète entre Microsoft, Sun Microsystems et Cisco. La faille, une possibilité de router n'importe quelle adresse Internet légitime vers n'importe quel serveur. Autant dire du bain béni pour les pirates. La faille a été découverte totalement par hasard, il y a six mois, par un spécialiste en sécurité, Dan Kaminsky, ingénieur chez IO Active. « Aucune opération de sécurité n'a jamais été réalisée à cette échelle », a-t-il déclaré à l'AFP. Guillaume Lovet, expert en cybercriminalité, responsable de l'équipe anti-menaces chez Fortinet précise : « l'origine de la faille vient du protocole « DNS » (Domain Name System) qui a été défini en 1983, quand internet n'était pas appelé à devenir ce qu'il est aujourd'hui en terme d'importance du réseau. La sécurité et l'authentification des informations ne sont donc pas inscrites dans le design d'Internet ce qui explique les problèmes de cybercriminalité et notamment l'arrivée des spams. Ce n'est pas la première fois qu'il y a une faille comme celle-ci, mais avant le phénomène du phishing n'avait pas la même ampleur qu'aujourd'hui. La rustine mise en place par les géants de l'informatique est une solution à court terme, mais la solution à long terme serait donc de re-définir les protocoles clef de l'Internet, ce qui est long et très coûteux ».

UN ROBOT PATROUILLEUR DANS L'ENTREPRISE...

Voici venir le premier robot capable de dire si un employé est en train de frauder sur ses heures de bureau. Au Japon, les employés déclarent eux mêmes leurs heures supplémentaires. Bilan, certains salariés indiquent travailler des dizaines d'heures en plus alors que cela n'est pas vrai. Que cela ne tienne, la société Duskine, une société de location vient de signer la location d'un robot contrôleur. Pour 2.300 € par mois, l'entreprise fait appel au robot Alsok. Le robot va se promener dans les bureaux de l'entreprise afin de contrôler les salariés. Ces derniers doivent présenter leur badge afin d'être pointés. «Il sait même prendre seul un ascenseur pour explorer tous les étages» explique l'agence Belga.



LA NUIT DES MORTS VIVANTS POUR L'ADMINISTRATION BUSH

Le Social Security Administration (SSA), l'une des administrations les plus importantes sur le territoire américain, vient de révéler que plusieurs processus internes s'étaient mal déroulés au sein de ses services. 20 000 informations privées de

citoyens américains se sont retrouvées potentiellement divulguées dans le fichier Death Master File, un document regroupant les personnes décédées durant l'année. Sur les 2,5 millions de défunts recensés pour l'année 2007 figuraient en effet 20 000 Américains bien vivants. Bilan de la boulette : leurs informations sensibles, dont le fameux Social Security Number, un sésame qui permet, aux États-Unis, d'ouvrir un compte en banque ou encore de demander un crédit, se sont retrouvées en accès libre.

POP-CORN CUIT PAR DES TÉLÉPHONES PORTABLES : BIDON !

En juin dernier une vidéo virale avaient tenté de prouver que des téléphones portables étaient capable de cuire des pop-corn. Le buzz avait fait le tour de la planète en enregistrant 16 millions de spectateurs sur Youtube. Les vidéos montraient l'explosion

DES PIRATES DANS LES DISTRIBUTEURS DE BILLETS

Des pirates informatiques ont réussi à pénétrer dans le réseau des distributeurs de billets (ATM - Automated Teller Machine) appartenant à la Citibank. Les intrus sont passés par les magasins 7-eleven et ont réussi à dérober des codes confidentiels appartenant aux clients. Les pirates ont ciblé l'infrastructure du système ATM qui fonctionnait sous Windows. Bilan, il semble que les pirates aient trouvé LE passage aux données sensibles. Ils ont pu profiter d'un problème de chiffrement de certains ATM. La faille aurait permis d'intercepter les codes au moment où ces derniers passaient entre l'ATM et les ordinateurs qui traitaient les transactions.



de grains de maïs en pop-corn sous l'effet présumé de téléphones portables. Des doutes étaient rapidement survenus. Et pour cause puisque l'on sait aujourd'hui que sous la table se serait caché un Magnétron retiré d'un four à micro onde. La société à l'origine de ce buzz, Cardo Systems, commercialise des oreillettes bluetooth. Espérons surtout, pour les acteurs de ce canular, que les électrons diffusés par le Magnétron ne leur ont pas grillés le peu de méninges dont ils disposaient encore...

CANAL + DIFFUSE GRATUITEMENT SES ÉMISSIONS SUR INTERNET



Voilà une erreur assez étonnante de la part de la chaîne à péage Canal Plus. Durant une petite semaine, début juillet, la télévision à péage a diffusé ses films, gratuitement, à partir de l'Internet. Une erreur de taille. Il suffisait de cliquer sur le lien iTV, sur le site officiel de Canal, plus pour se retrouver avec Canal + décrypté et sans payer le moindre droit de passage et cela via Windows MP ou VLC. Plusieurs webmasteurs avaient trouvé là un bon filon en diffusant, sur leurs sites, le précieux lien.

YOUTUBE CONTRAIT À BALANCER...

La société Viacom, plateforme de diffusion d'émissions de télévision, semble avoir gagné une victoire, début juillet à l'encontre du portail communautaire de diffusion Youtube. Viacom accuse, depuis 2007, la filiale de Google de participer à la «violation massive et intentionnelle des droits d'auteur». Viacom réclame un milliard de dollars de dommages et intérêts. Un tribunal américain vient de donner raison à Viacom et a demandé à Youtube de communiquer toutes les données concernant ses utilisateurs: Logs, adresses IP, dates de connexion, ... L'Electronic Frontier Foundation (EFF) n'a pas tardé à réagir: «Le jugement est un retour en arrière pour les droits à la vie privée, et permettra à Viacom de voir tout ce que vous consultez sur YouTube.»



PLUS AUCUNE TRACE !

Vous avez des documents sensibles sur votre disque dur ? Vous devez les supprimer en toute hâte ? Pas de panique, suivez le guide !

Parfois, supprimer les fichiers et vider ensuite la corbeille de Vista ne suffit pas. Imaginons que vous souhaitiez revendre votre PC. Vous n'apprécieriez certes pas que quelqu'un puisse récupérer les documents sur lesquels vous aviez travaillé, pas vrai ? Pour éviter tout risque, il vous faut donc un mode de suppression totalement sécurisé. Une opération qui n'est pas prévue par Vista et que vous allez donc devoir effectuer en utilisant d'autres programmes. Mais attention, ne prenez pas n'importe lesquels, car la moindre erreur pourrait rendre une partition totalement inutilisable, voire même tout le disque dur dans le pire des cas.

:: Contrôlez le bas niveau

On trouve sur Internet de nombreux programmes susceptibles de nous venir en aide tant pour supprimer des fichiers en toute sécurité que pour effectuer un formatage total du disque dur, rendant vaine toute tentative de récupération des données.

LES PROGRAMMES UTILES

CCLEANER 2.03.532

Gratuit
www.ccleaner.com

FILE SHREDDER 5.5

Gratuit
www.handybits.com

SURE DELETE 5.1.1

Gratuit
www.wizard-industries.com

ULTIMATE BOOT CD

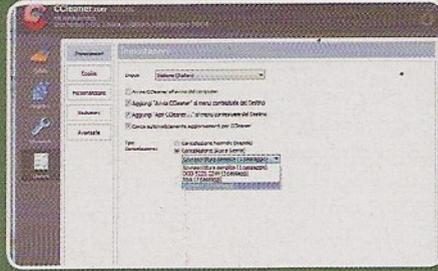
Gratuit
www.ubcd4win.com

CLEANER



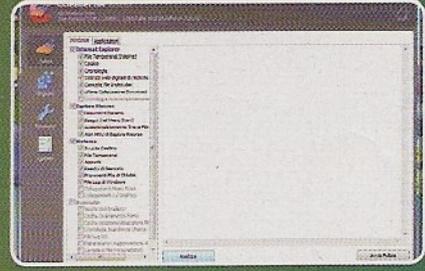
1 LANCEZ-LE À PARTIR DE LA CORBEILLE

Téléchargez puis exécutez CCleaner à partir de www.ccleaner.com. Cliquez ensuite avec le bouton droit sur la Corbeille de Vista et sélectionnez Ouvrir CCleaner.



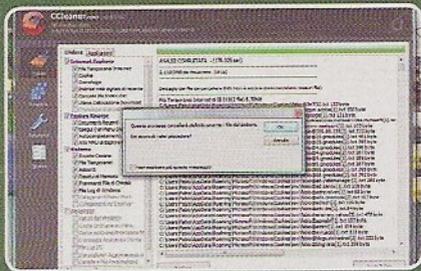
2 CHOISISSEZ LE NIVEAU DE SÉCURITÉ

Pour activer le mode de Suppression Sécurisée, ouvrez les Options et, dans Paramètres, choisissez Suppression par réécriture. Le mode Gutmann est très lent.



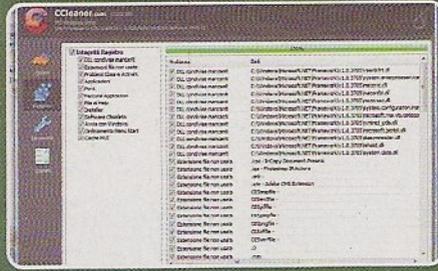
3 CONTRÔLEZ PUIS NETTOYEZ VOTRE PC

À présent, allez dans l'onglet Nettoyage et contrôlez les éléments à supprimer dans la section Windows. Enfin, cliquez sur Analyser pour lancer la procédure de lecture du disque dur.



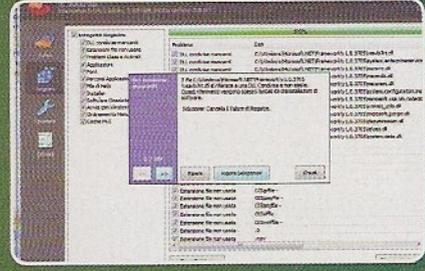
4 ET MAINTENANT... SUPPRIMEZ TOUT !

Une fois la phase d'analyse terminée, le programme listera tous les fichiers que vous pouvez supprimer en totalité. Pour confirmer l'opération de suppression, cliquez sur Lancer le Nettoyage.



5 NETTOYEZ AUSSI LE REGISTRE

Vous pouvez aussi utiliser CCleaner pour supprimer les données contenues dans le Registre système. Allez à présent dans l'onglet Registre et cliquez sur Trouver des Problèmes.



6 RESTAUREZ L'INTÉGRITÉ DU SYSTÈME

Toutes les erreurs trouvées seront automatiquement corrigées et les correspondances manquantes seront supprimées. Terminez la procédure en cliquant sur Réparer les erreurs sélectionnées.

Une activité plus connue sous le nom LLF ou Low Level Format, à savoir formatage à bas niveau. Il y a dix ans à peine, le formatage à bas niveau était l'une des nombreuses options proposées par le BIOS de la carte mère. Aujourd'hui en revanche, on peut l'effectuer avec des programmes spéciaux proposés par les fabricants des disques eux-mêmes sur leur site Internet. Le formatage à bas niveau présente toutefois un inconvénient pour le moins déplaisant : il contribue à diminuer la durée de vie du disque dur. Pourquoi ? Parce qu'il ne se limite pas à supprimer les données, mais agit directement sur la couche magnétique qui

contient les informations. Plus la magnétisation est altérée ou modifiée, et plus vous avez de chances de voir certains points se démagnétiser en créant ainsi des zones non utilisables : les fameux "bad cluster".

:: Supprimés oui, mais pour de faux !

Pour bien comprendre comment supprimer définitivement des données, voyons d'abord comment s'effectue une suppression classique. Chaque disque dur contient un tableau de correspondance entre le nom de cha-

que fichier et dossier et la position de chaque partie ou cluster qui les composent. Lorsqu'on supprime un fichier, les clusters ne sont pas détruits matériellement parlant. Seule est interrompue la correspondance entre le nom du fichier et la position des éléments qui le constituent. Un signe conventionnel est inséré, habituellement un point d'interrogation ou un tilde, en remplacement de la première lettre du nom du fichier ou du dossier à l'intérieur du tableau de correspondance. Tous les éléments présentant un point d'interrogation ou un tilde au sein du Tableau de correspondance du Fichier Systè-

me, sont considérés comme supprimés du système d'exploitation. Toutefois, les données enregistrées dans les clusters sont encore matériellement disponibles jusqu'à être écrasées.

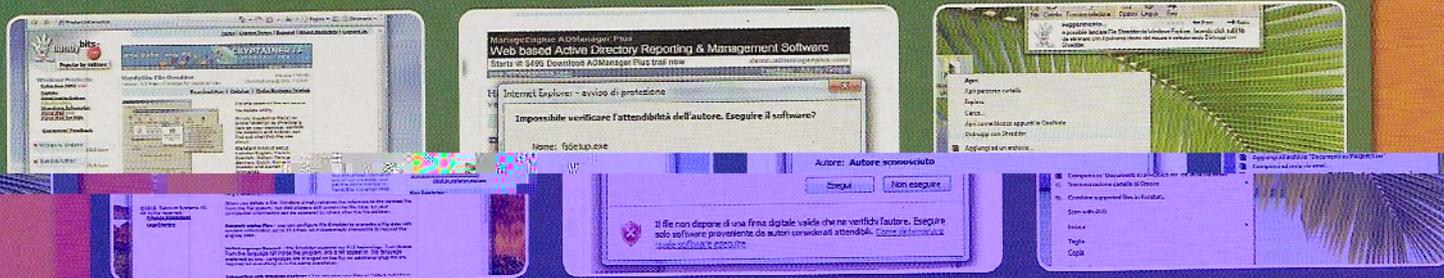
:: Couche sur couche

Pour obtenir une suppression définitive, les données d'origine doivent être écrasées une ou plusieurs fois par d'autres données aléatoires. Plus les données d'origine seront écrasées, et moins vous aurez de chances de les récupérer. Les méthodes de suppression sécurisée sont classées selon le nombre de passages effectués : la ré-écriture simple prévoit un seul passage, DOD 5220.22-M trois passages, NSA ou National Security Agency sept passages et enfin Gutmann, 35 passages. Le temps nécessaire pour supprimer à jamais les données dépendra du nombre de passages choisi pour la ré-écriture de ces données. Certains programmes de suppression sécurisée des données utilisent l'un des standards de ré-écriture universellement reconnus. D'autres, comme

File Shredder 5.5, développé par Handybits, www.handybits.com, permettent de sélectionner comme bon vous semble le nombre de passages sur une échelle allant de 1 à 15. Attention toutefois : en cas de désinstallation, ce programme laisse un autre petit programme appelé Teknum System, qui permet de rechercher les mises à jour sur Internet. Ce qui est pour le moins gênant, même s'il ne s'agit en aucun cas d'un spyware. Pour l'effacer, il suffit d'utiliser la fonction Gestion des programmes de Windows Defender, en le supprimant à partir de la rubrique Programmes exécutés automatiquement.

me, sont considérés comme supprimés du système d'exploitation. Toutefois, les données enregistrées dans les clusters sont encore matériellement disponibles jusqu'à être écrasées.

INSTALLER ET CONFIGURER DES FICHIERS



1 CA MARCHE AUSSI AVEC VISTA !

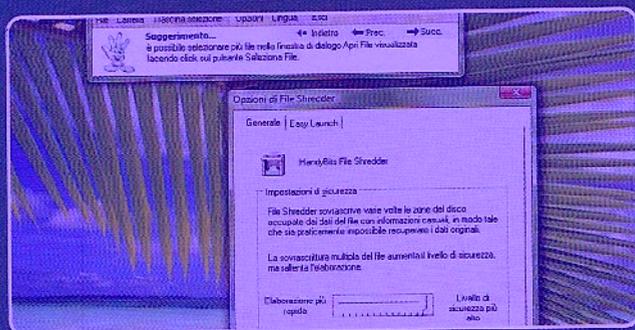
Vous trouverez le programme File Shredder 5.5 sur www.handybits.com. Développé à l'origine pour Windows XP, il fonctionne aussi sans encombre sous Vista.

2 UTILE MAIS INSIDIEUX

File Shredder installe aussi Teknum System. Vous pouvez effacer ce programme avec Windows Defender, en le supprimant de la rubrique Exécution automatique de Programmes.

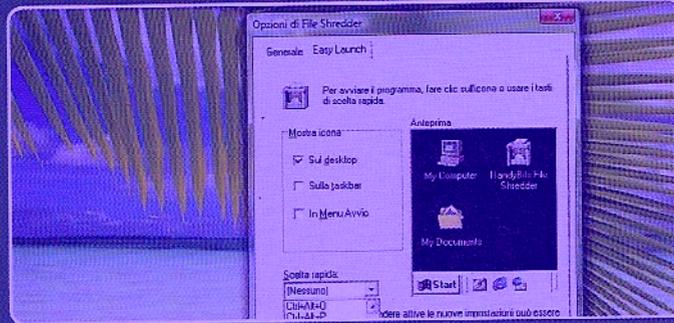
3 UTILISEZ-LE COMME BON VOUS SEMBLE

Vous pouvez utiliser File Shredder en faisant glisser dans la fenêtre du programme les fichiers que vous souhaitez supprimer, ou en cliquant avec le bouton droit sur les documents à supprimer.



4 CHOISISSEZ LE NIVEAU DE SÉCURITÉ

Pour paramétrer le nombre de ré-écritures que vous souhaitez exécuter pour sécuriser la suppression, ouvrez le menu Options et indiquez un chiffre entre 1 et 15 dans Paramètres de sécurité.



5 TOUJOURS DISPONIBLE

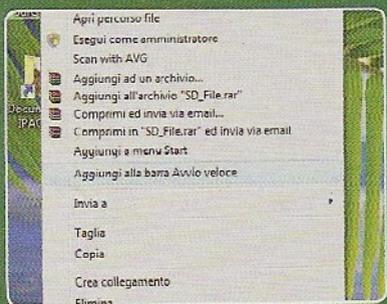
Si vous n'aimez pas la fenêtre du programme qui s'ouvre sur le bureau de Vista, vous pouvez toujours utiliser l'onglet EasyLaunch pour configurer l'emplacement de l'icône ou les touches de Sélection rapide.

FORMATEZ AVANT DE VENDRE

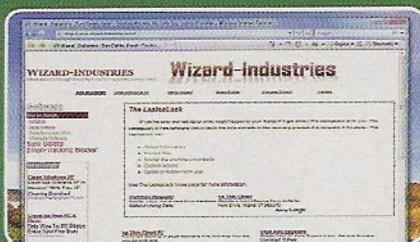
Vous avez décidé de donner ou de vendre votre vieux PC ? Alors veillez auparavant à supprimer vos fichiers et documents personnels à l'aide d'un programme de formatage à bas niveau. Si le fabricant du disque dur ne fournit pas le programme nécessaire à cette opération, vous pouvez graver un CD de boot spécial en utilisant les options du programme Ultimate Boot CD, <http://www.ubcd4win.com>. Grâce à sa procédure guidée, vous allez pouvoir réaliser un disque de boot capable d'activer le formatage à bas niveau de n'importe quel disque dur. Mais avant de créer le CD et de l'utiliser sur votre ordinateur, assurez-vous de bien avoir enregistré tous les documents importants : car une fois le formatage achevé, votre disque dur redeviendra totalement vierge !

DEUX CORBEILLES

Sure Delete 5.1.1 ajoute une seconde Corbeille au bureau de Windows, à utiliser pour supprimer définitivement du disque dur les fichiers les plus confidentiels. En cliquant avec le bouton droit sur l'icône SureDelete, deux options s'affichent : Ajouter au menu Démarrer et Ajouter à la barre de Lancement rapide. La sélection d'une ou des deux options vous permet de déplacer l'icône du programme dans les emplacements respectifs.

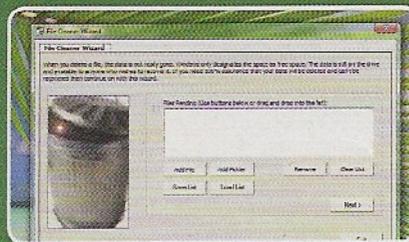


UNE NOUVELLE CORBEILLE AVEC SURE DELETE



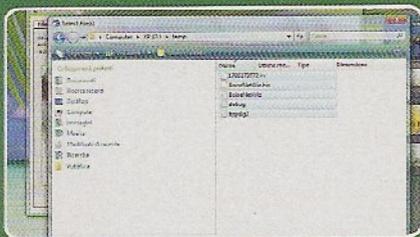
1 TROUVEZ LE PROGRAMME

On ne peut pas dire que la page de Wizard Industries, www.wizard-industries.com, où télécharger Sure Delete 5.1.1 soit très bien faite. Parcourez-la jusqu'à trouver le nom du programme puis téléchargez-le.



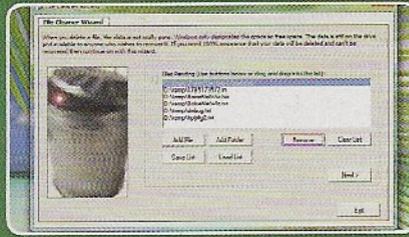
2 SUIVEZ LES DIFFÉRENTES ÉTAPES

Une fois l'installation terminée, sur le bureau de Vista apparaîtra la nouvelle corbeille intitulée Sure Delete. La procédure de suppression sécurisée des données s'activera simultanément.



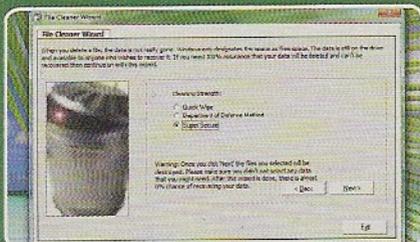
3 SÉLECTIONNEZ LES FICHIERS À SUPPRIMER

La fenêtre Select File(s) s'ouvrira en cliquant sur Add File. Sélectionnez tous les documents que vous souhaitez supprimer puis cliquez sur Ouvrir, en bas dans la fenêtre.



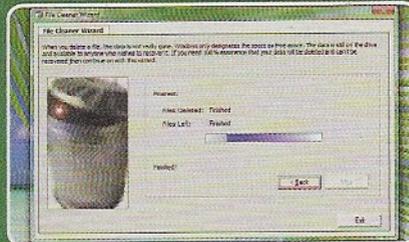
4 CORRIGEZ LES ERREURS ÉVENTUELLES

Si, pendant votre choix, vous avez aussi indiqué des fichiers que vous souhaitez en revanche garder, vous pouvez les sélectionner et utiliser le bouton Remove après être revenu à la fenêtre principale. À la fin, cliquez sur Next.



5 RAPIDE... OU SUPER SÛR ?

Sure Delete n'indique pas le nombre de ré-écritures qui seront effectuées par le programme, mais permet de choisir parmi trois niveaux. Le premier est le plus rapide, le dernier étant le plus sûr.



6 SUPPRIMEZ À JAMAIS VOS FICHIERS

Après avoir cliqué sur Next, la suppression totale des données démarrera. Le temps nécessaire dépend du niveau choisi et du nombre de fichiers sélectionnés.

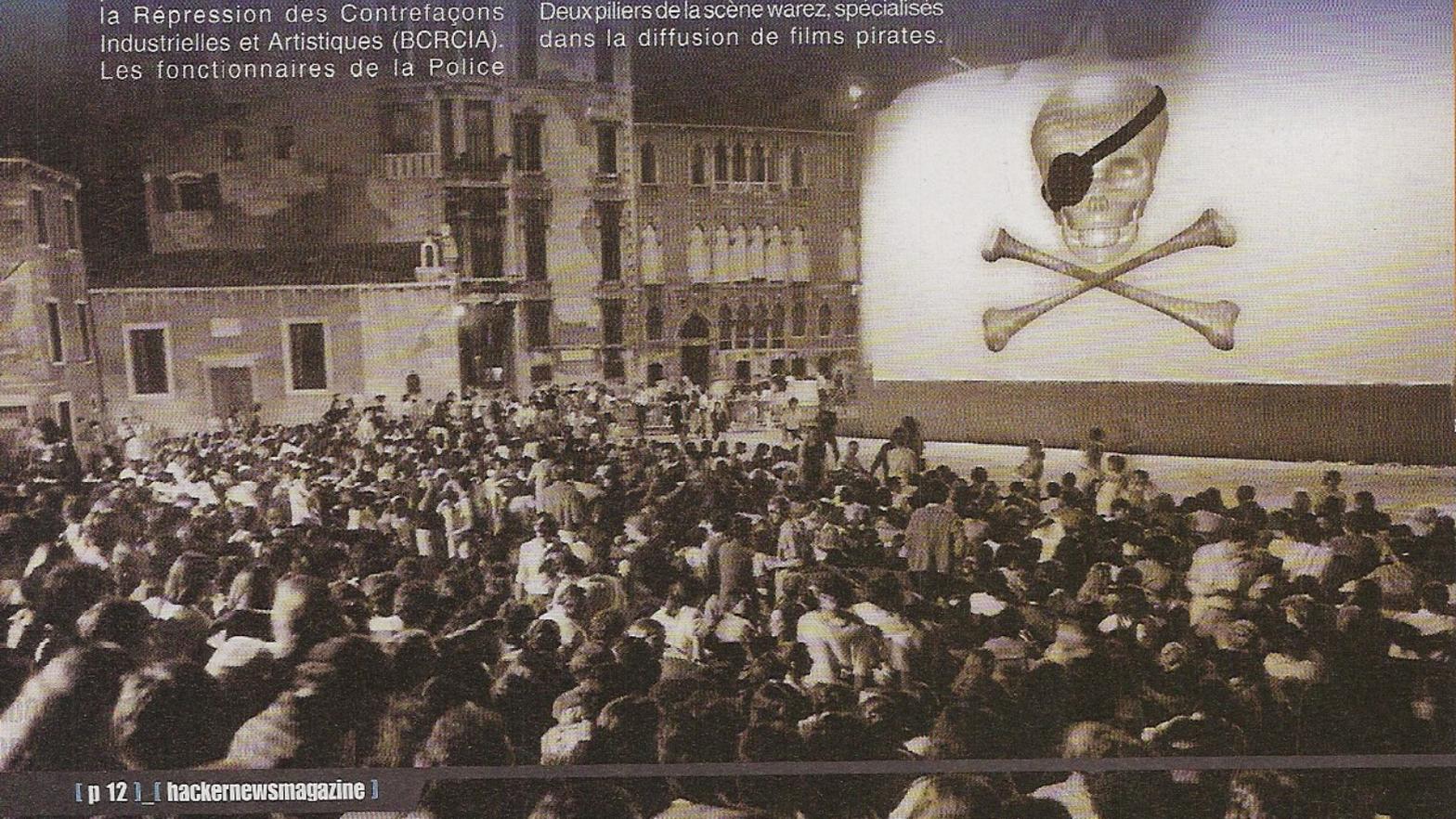
Le WAREZ francophone en danger ?

Fin juin, la police française a mis la main sur plusieurs importants membres de deux groupes warez, Cinefox et CaRNage. Panique chez les pros de la contrefaçon et les petits copieurs en mal de nouveautés.

À la fin du mois de juin n'aura pas été propice qu'aux passages d'examens en tout genre. On peut même dire que le prix d'excellence pourra être remis aux policiers de la Brigade Centrale pour la Répression des Contrefaçons Industrielles et Artistiques (BCRCIA). Les fonctionnaires de la Police

Judiciaire ont attrapé, coup sur coup, quatre internautes pas comme les autres. D'abord les administrateurs du groupe Cinefox, puis un membre important de la team connue sous le pseudonyme de CaRNage. Deux piliers de la scène warez, spécialisés dans la diffusion de films pirates.

Les policiers ont réussi à remonter la piste de Cinefox à partir d'un mystérieux document diffusé sur Internet en août 2007. Le fichier texte, baptisé Bustme, mettait à jour les ips, les pseudonymes, les accès aux serveurs



Ftp, aux serveurs IRC ainsi qu'au code permettant de déchiffrer les messages diffusés. Bref, une manne providentielle pour toute personne souhaitant gratter la vernis de ce type de société numérique. L'enquête de la BCRGIA s'est focalisée sur les responsables d'un serveur warez, mais aussi sur l'individu qui allait « voler » les films en salle de cinéma. « Un bel exemple de criminalité en bande organisée, facteur aggravant en matière de contrefaçon » va confirmer une source proche du dossier. L'individu qui se rendait dans les cinémas pour enregistrer les films illégalement fournissait principalement ses « productions » à Cinefox, mais il signalait ses méfaits sous d'autres pseudonymes. Cinefox, par exemple, va signer un grand nombre de copies sous différents pseudos, GeT, QTRF, ...



Au dernier relevé, le groupe Cinefox avait diffusé plus de 200 « releases » pirates françaises en tous genres (camcord, DVD screener, R5, Blu-Ray) en quelques mois. Rien que sur Mininova, 246 torrents sont référencés. Pour rappel, Cinefox ne diffusait pas ses « créations » sur le P2P mais via des TOPSites, des espaces clos, très restrictifs où seule les personnes habilitées peuvent accéder. « La saisie du matériel informatique des personnes arrêtées, explique l'Association de Lutte contre le Piratage Audiovisuel, devrait permettre d'identifier de nouvelles cibles car on sait que les différents teams pirates sont fréquemment en contact. Quelques personnes ont été arrêtées pour l'instant, mais il s'agit de cibles prioritaires. On espère que d'autres suivront. » Un membre d'un de ces topsites nous a

expliqué ce qui avait bien pu se passer « L'histoire est parti du fait qu'un siteop (un administrateur de serveur warez, un top, NDR) est venu piquer des affils (Des membres du Top, NDR) à un autre siteop (...) Des sites comme ceux balancés rapportent énormément d'argent (...) et quand c'est des teams qui louent ces accès, ça leur permet de payer tout leur supply (Ceux qui diffusent dans les top, NDR) (...) Le mec qui prend le son en salle, faut bien le payer, ce n'est pas gratuit, surtout pour des bandes comme ça (...) en même temps ça leur fait de l'argent de poche (...) J'ai déjà vu un siteop se faire plus d'argent qu'un ouvrier (...) ces gens là sont condamnés sur la scène. (...) Les informations publiées sont vieilles, 80 % des slaves on été changés, le Dns ne pointe pas du tout vers l'ip inscrite. (...) Une erreur qui donne des précisions sur le corbeau ».

Cinefox fournissait donc aussi beaucoup d'images. Son fondateur, connu aussi sous le pseudonyme de Gandja/Wereld (WeR - VFC/SCaN) participait à d'autres groupes comme GeT. Des partenariats avec d'autres teams. Des échanges de bons procédés comme avec l'ex team AAV (En fait VCDFry) auprès de qui il récupérait des sons afin de fabriquer des « productions » francophones.

;; Le warez francophone mis à mal ?

La seconde opération policière a visé une team qui prenait de plus en plus de puissance dans le milieu warez. CaRNage diffusait énormément de nouveautés filmées en salle. L'opération menée à Montpellier, comme pour l'un des membres de Cinefox, a décapité un autre maillon de la chaîne warez francophone. Le membre de CaRNage était spécialisé dans le camcording de films (filmer illégalement au caméscope des films lors de leur projection en salle, NDR). Il était notamment l'origine de toutes premières versions pirates françaises de films

tels que « Asterix Aux Jeux Olympiques », « Jumper », « Bienvenue Chez Les Chtis », « Iron Man », « Indiana Jones And The Kingdom Of The Crystal Skull », « Skate or Die » ou encore « Phénomènes ». Les cyber-policiers sont particulièrement actifs ces derniers temps et la moisson pourrait bien continuer. Les personnes interpellées ont fourni des renseignements permettant de remonter à d'autres pirates professionnels, dont certains se trouvent au Canada, en Hollande, Suisse et Belgique. Les personnes interpellées « ont reconnu les faits ». Elles ont de quoi se faire du souci car les œuvres qu'ils diffusaient illégalement sur Internet étaient essentiellement des nouveautés en cours d'exploitation en salles ou non encore sorties en France. Les ayants droit lésés pourraient donc fort logiquement chercher à réclamer des comptes à ces pirates, en plus de la procédure pénale qui est déjà en cours suite à l'ouverture d'une information judiciaire auprès de la juge d'instruction Mme JUVASINOVIC (TGI de PARIS). « Compte tenu de l'ampleur des films présents et du matériel saisi, indique un proche du dossier, un décompte précis n'a pu être réalisé à ce stade des opérations, mais plusieurs milliers d'œuvres sont concernées ». L'enquête va maintenant se poursuivre à partir de nombreuses identifications relevées lors des perquisitions menées aux domiciles des personnes interpellées. De nombreux serveurs ont été identifiés lors de l'enquête. Certains espaces de stockage pouvaient atteindre 60 Tera octets de données, soit environ 88 000 films au format DivX. ■



L'armée se prépare à une cyberguerre



Après la Chine, Taïwan, les États-Unis, l'Otan... voici que la France décide de se lancer dans la course à la cyberarmée. Sommes-nous si proches que ça d'un cyberconflit ?

Le livre blanc de la défense présenter par Nicolas Sarkozy, en juin dernier, mettait en avant un intérêt certain à se préparer à une cyberguerre. Ce livre blanc de la défense annonçait le besoin d'acquérir des satellites d'observation et d'espionnage, via des écoutes électromagnétiques par exemple. L'hexagone souhaite aussi se doter de capacités de lutte informatique offensive. Des cyberguerriers qui seront dirigés par l'état-major des armées. Les services de renseignements ne devraient pas être dépourvus de cette capacité à répondre à des tentatives d'attaques informatiques. La France, en retard d'un wagon ? Oui et non. Il faut dire aussi que des pays comme la Chine ou encore les États-Unis ont réfléchi au problème depuis une décennie. En 1999, deux colonels de l'armée Chinoise écrivaient déjà un document sur l'innovation de la technologie pour remporter une guerre. Finalité du rapport, remporter une victoire sans se battre. C'est un février 1999 que deux colonels de l'armée Chinoise, à savoir Qiao Liang et Wang Xiangsui, diffusé une étude sur les développements futurs et le potentiel d'une guerre asymétrique. Bref, comment remporter une guerre sans sortir

le moindre fusil. Les auteurs indiquaient d'ailleurs une méthode qui a touché les USA, l'Angleterre, la France aussi, depuis une année : "Cent victoires lors de cent batailles n'est pas des plus adroit. Le fait de piéger son ennemi sans bataille est le plus intelligent." Le document était intitulé "Unrestricted Warfare", il mettait clairement, noir sur blanc, les différentes guerres à contrôler : informatiques, économiques, financières, ... (<http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>)

OTAN en emporte le vent !

Décembre 2006, l'Estonie, à la suite d'une série d'attaques informatiques, proposait la mise en place et l'hébergement d'un centre dédié à la cyberdéfense des intérêts des membres de l'Otan. "L'objectif du centre serait de promouvoir la coopération entre les membres de l'Otan dans la défense informatique, de préparer des programmes de formation et de travailler sur les aspects légaux de la lutte contre le cyber-terrorisme", expliquait à l'époque Lauri Allmann,

sous-secrétaire au ministère Estonien de la défense. Pas vraiment une unité de cybersoldats, mais plutôt un centre de "conception". Deux ans plus tard, le centre prenait vie dans une bâtiment militaire situé à Tallin. Le bâtiment, constitué de grosse pierre de taille claire, au style Vauban, va recevoir ce centre pas comme les autres. Suleyman Anil, en charge de la sécurité informatique à l'OTAN, expliquait lors de la conférence E-Crime congress de Londres que le piratage informatique était devenu une des inquiétudes de l'Organisation du Traité de l'Atlantique Nord. L'espionnage en ligne et l'e-terrorisme représentant maintenant de vraies menaces « Le piratage informatique est maintenant mentionnée au plus haut niveau avec les attaques de missiles et l'énergie. Ces attaques sont de plus en plus nombreuses, nous ne croyons pas que ce problème disparaisse rapidement à moins que des mesures à l'échelle mondiale soient prises. Le piratage informatique peut devenir un problème global." Un message clair à l'encontre des pirates et des Etats qui auraient la prétention de cautionné des pirates électroniques Un second centre se monte aussi, en parallèle de celui de Tallin. Le Centre d'excellence de l'Otan pour la défense cybernétique, s'est installé au siège de l'Otan, à Bruxelles. ■



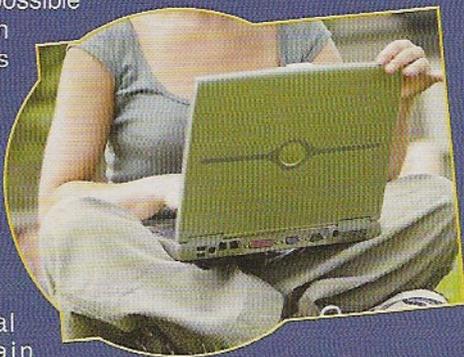
Vol de données privées : ça n'arrive pas qu'aux autres !

Les universités américaines sont en passe de remporter le trophée HNM de la passoire numérique ! Un régal pour les pirates des campus...



Pendant que certains campus américains coupent les connexions de leurs étudiants un peu trop friands de musique piratée, les mêmes universités oublient un point important...

surveiller aussi attentivement leurs portes d'entrée. Depuis plusieurs semaines, pas une journée sans une alerte électronique. Les pirates ont parfaitement compris que dans les serveurs des écoles de l'Oncle Sam il était possible de trouver bien autre chose que des cours et des notes. Par exemple, des données confidentielles comme le numéro de sécurité social. Rien à voir avec le numéro français. Le Security Social Number américain permet, notamment, d'ouvrir un compte en banque, de se faire rembourser des impôts trop payés... bref, un outil parfait pour un escroc souhaitant usurper une identité.



Celle qui gagne le pompon, c'est l'Université de Californie qui a déjà à son passif plusieurs piratages dont un particulièrement mémorable : la ponction de 800 000 dossiers d'étudiants en un

an ! Nous avons recensé, via la presse américaine, pas moins de 96 cas, rien qu'au premier trimestre 2008. Dernier cas en date, l'université d'Antioch (Ohio) qui « perdait » 70 000 données appartenant aux étudiants et aux personnels de l'école en avril dernier. Même chose pour l'Université d'Oklahoma. Le pirate est passé par le serveur de gestion des parkings de l'école. Même la prestigieuse Harvard a subi une frappe chirurgicale.

En février, un pirate diffusait sur le P2P 125 Mo de données appartenant à l'école. Le plus étonnant est que la police fédérale américaine avait incité les présidents d'universités à devenir les yeux et les oreilles de l'Oncle Sam pour contrer... les terroristes et les espions. Le Comité consultatif d'Enseignement supérieur de la Sécurité Nationale, installé en 2005 (<http://www.fbi.gov/pressrel/pressrel05/highed091505.htm>), se compose d'une vingtaine de présidents d'universités du pays. Les responsables de ces "facs" travaillent avec le FBI sur des questions liées à la sécurité des campus, le contre-terrorisme et coincer d'éventuels espions

et autres recruteurs. Selon le rapport de la NPR (<http://www.npr.org/templates/story/story.php?storyId=16067492>), le FBI conseille aux membres de penser comme aux temps de la "Guerre Froide". Aux directeurs de surveiller les professeurs et les étudiants qui seraient susceptibles d'être sur le campus à des fins d'espionnage, de vol d'informations liées à des recherches universitaires ou en vue de recruter des étudiants qui auraient des sympathies à une cause anti-américaine. À première vue, il y a encore du travail sur la table !

:: Portes ouvertes

En mars dernier, l'université de Genève (Suisse) se retrouvait avec une fuite de données appartenant à de futurs étudiants de la section théologie de l'école. Heureusement, pour son cas, un hacker est passé par là et a pu aider à corriger ce « bug » qui permettait d'intercepter noms, adresses, téléphones, ... des élèves. En France, tout semble être nickel. Enfin presque. La Sorbonne avait été piratée en 2006 par un défacteur connu sous le pseudonyme de Furtivo (Xtech Crew). Même aide pour l'université Claude Bernard de Lyon. Un accès aux données privées des nouveaux et anciens élèves. Prévenus, les administrateurs de la faculté ont rapidement corrigé.

ATTAQUE VIRALE *par* *site* INTERPOSÉ

Certains pirates ont de la suite dans les idées et des idées pour s'incruster dans nos ordinateurs. Après la diffusion de virus par courrier électronique, via des logiciels balancés sur le P2P, voici l'infection au travers de sites Internet ayant pignon sur web. Attention, personne ne semble être à l'abri.

Depuis plusieurs mois, une petite dizaine de groupes de pirates particulièrement bien organisés tyrannisent Internet en s'attaquant à un énorme paquet sites grand public. Personne ne semble pouvoir leur échapper. MTV, Durex, MSNBC, plusieurs sites officiels du groupe AB, spécialisé dans la télévision par satellite. La méthode d'attaque semble simple et

particulièrement efficace. Les intrus en vont pas tout casser sur le site qu'ils ont pénétré. Ils préfèrent la jouer plus soft, plus vicieux. Ils utilisent pour cela un DIY (Do It Yourself - Faites-le vous-même, bref un logiciel fait maison) de type Asprox. Asprox, par exemple, utilise des DIY qui ont pour mission d'injecter des commandes SQL pour pirater des sites et leur installer des commandes malicieuses, comme

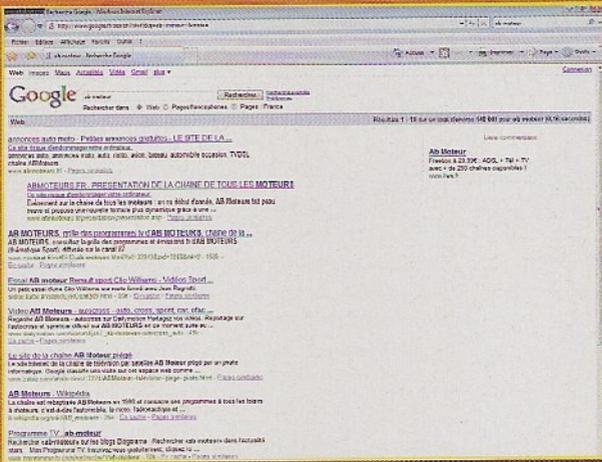
l'installation d'un logiciel espion. Le bot n'installe qu'une petite iframe dans le code source du site piégé et le tour est joué. "Concernant MTV France, explique un spécialiste du sujet, les injections SQL de masse ont été repérées et ont été corrigées rapidement. Là où il y a matière à réflexion, c'est que les injections ont touchés les deux principaux flux RSS, ce

qui bien eu un effet boule de neige puisque tous les utilisateurs des sites relayant les news ont pu être exposés aux exploits." Concrètement, rien de bien nouveau, ça prouve encore une fois qu'aucun site n'est digne de confiance mais les pirates ont bien vite compris l'intérêt de ce type d'attaque. Plus le site piégé est important, plus les victimes seront nombreuses.

:: Capote trouée

Fin mai, la marque internationale de préservatif ne pensait pas se retrouver avec un microbe dans ses entrailles numériques. Un de ces groupes avaient réussi à y injecter un iframe qui lançait le téléchargement d'un logiciel espion dans les ordinateurs des visiteurs. Une visite numérique pirate totalement transparente pour l'internaute, surtout si sa machine et ses logiciels de surfs (antivirus, navigateur, player flash, ...) n'avaient pas été mis à jour. Les attaques sont particulièrement poussées.





moteur, du groupe AB ont été victimes de ce type d'intrusion. Autant dire que les visiteurs des dits sites n'ont pas du apprécier l'humour. Un bon antivirus, même gratuit comme Avast permettait de détecter une tentative d'intrusion à partir de AB Moteur ou NT1. Le lien piégé renvoyait sur le site adsitelo.com sur lequel le pirate avait mis en action un espionnage. L'armée n'a pas été épargnée par cette attaque, ce

communément appelées Oday, des vulnérabilités que peu de gens connaissent. Pour tenter de palier ces attaques, un navigateur mis à jour, des logiciels permettant de profiter d'Internet corrigés, un firewall et un antivirus correctement configurés devraient suffire. Mais comme a pu nous le confirmer un employé d'une société de sécurité informatique "ça prouve encore une fois qu'aucun site n'est digne de confiance."

Un lecteur a pu découvrir que ce type d'attaque était aussi parti d'un site baptisé banner82.com, "C'est le b.js qui m'a mis la puce à l'oreille, s'amuse-t-il, l'injection SQL était codée en hexadécimale et listait toutes les tables, tous les champs de type texte et ajouté un appel javascript à cet URL. Dans les logs, on voyait les cookies des membres modifiés suite à ça via banner82=update suivi des autres informations du site." Nous vous le disons, des pirates qui ont de la suite dans les idées. ■

Les pirates mettant en œuvre une stratégie d'attaque et une organisation qui laisse pantois. Pour Durex, plusieurs sites émetteurs avaient été installés. Ils cachaient tous le logiciel espion.

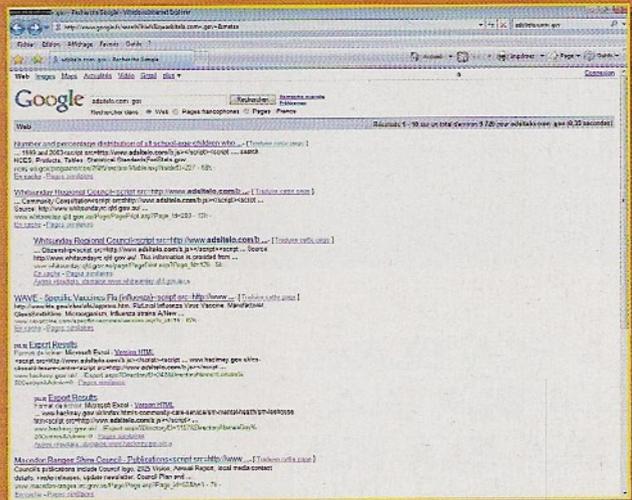
Les pirates ont d'ailleurs profité longuement d'une faille dans le logiciel Flash Player d'Adobe. Une vulnérabilité permettant de télécharger un logiciel espion dans la machine d'un internaute visiteur. Lors de l'attaque de fin mai, il s'est avéré que Durex n'était pas l'unique victime, mais plus de 10.000 sites différents. Certains injections ayant ratée, il suffisait de regarder Google référencer l'attaque. Parmi les victimes, l'encyclopédie en ligne de Microsoft (fr. encarta.msn.com), la CCI du VAR ou encore le site dédié à l'aéroport de Toulon-Hyeres.

Plus grave encore, des sites Internet de chaînes de télévision ont servi de support à ces attaques. Plusieurs télévisions par satellite et TNT, comme NT1, AB

des commanditaires. La Chambre de commerce et d'industrie de Paris, le Réseau d'information des droits de l'enfant ou encore un site de l'armée canadienne que les pirates ont tenté d'infiltrer. Même scénario, bot sql, iframe piégée dans les sites visés au hasard et des serveurs pièges ayant pour mission

Comment se protéger ?

Simple et compliqué à la fois. Ces pirates ont exploités des failles



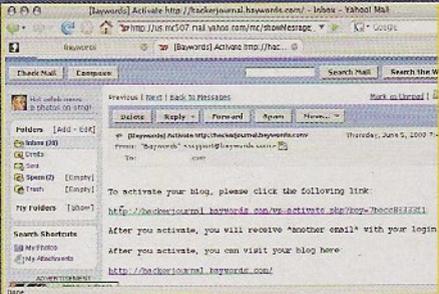


bouton "Next", en bas, une fenêtre s'ouvrira dans laquelle vous allez devoir choisir le nom du blog et le nom du sous-domaine (du type nomdublog.baywords.com).

Là encore, une option s'offre à vous, et vous propose cette fois d'indexer votre blog sur les moteurs de recherche spécifiques, à savoir Google et Technorati. La troisième et dernière fenêtre confirme la création de votre blog mais vous avertit



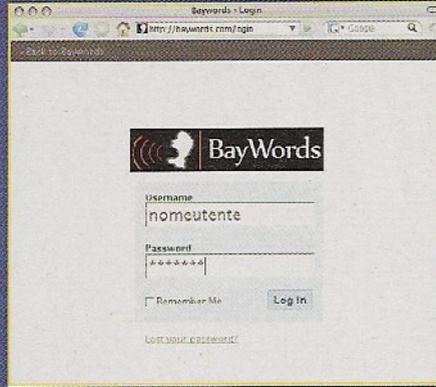
que pour le remplir, vous allez d'abord devoir l'activer à l'aide du lien contenu dans le message qui vous a été envoyé à l'adresse e-mail donnée. L'activation doit s'effectuer dans les 48 heures, sinon, toute la procédure d'enregistrement est annulée et vous allez devoir tout recommencer depuis le début !



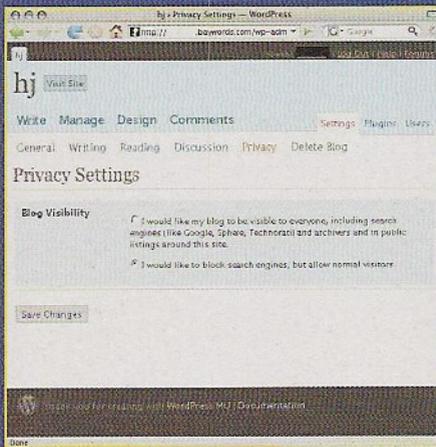
BayPress

En cliquant sur l'adresse contenue dans le message, vous allez être redirigé vers une fenêtre vous confirmant l'activation de votre blog et vous expliquant que vous allez

pouvoir vous connecter à l'aide du nom d'utilisateur choisi et d'un mot de passe, qui sera toujours envoyé par e-mail.



Dès la procédure d'enregistrement, différents éléments vous dévoilent la plate-forme adoptée par les Suédois mais les choses se clarifient dès l'apparition de la fenêtre de login : les blogs de chez Baywords sont basés sur le célèbre WordPress dans sa variante MU (<http://mu.wordpress.org/>).

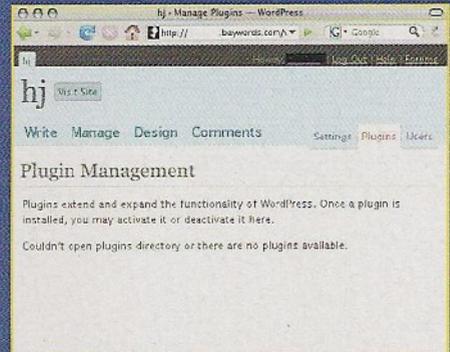


La version de WordPress adoptée est la 2.5, avec tous les outils nécessaires pour bichonner son blog : écrire des posts comme des pages, rédiger un blogroll, gérer des contenus, des commentaires et des mots-clés (les tags) et des catégories thématiques mais aussi des images et autres fichiers multimedia. Vous pouvez bien évidemment modifier l'aspect général à l'aide des 36 thèmes fournis. Si certains s'y sentiront un peu à l'étroit, pour les autres, les 100 Mo d'espace fournis sur le serveur s'avèrent plus que suffisants. A noter aussi, la possibilité, à partir

de son nom d'utilisateur, de créer et d'associer d'autres blogs, avec des adresses différentes, sur le serveur baywords.com.

Les limites

A bien y regarder, la seule limite de la plate-forme baywords concerne l'impossibilité d'installer de nouveaux thèmes ou de les modifier (en insérant par exemple un code personnalisé), et l'absence de plug-in.



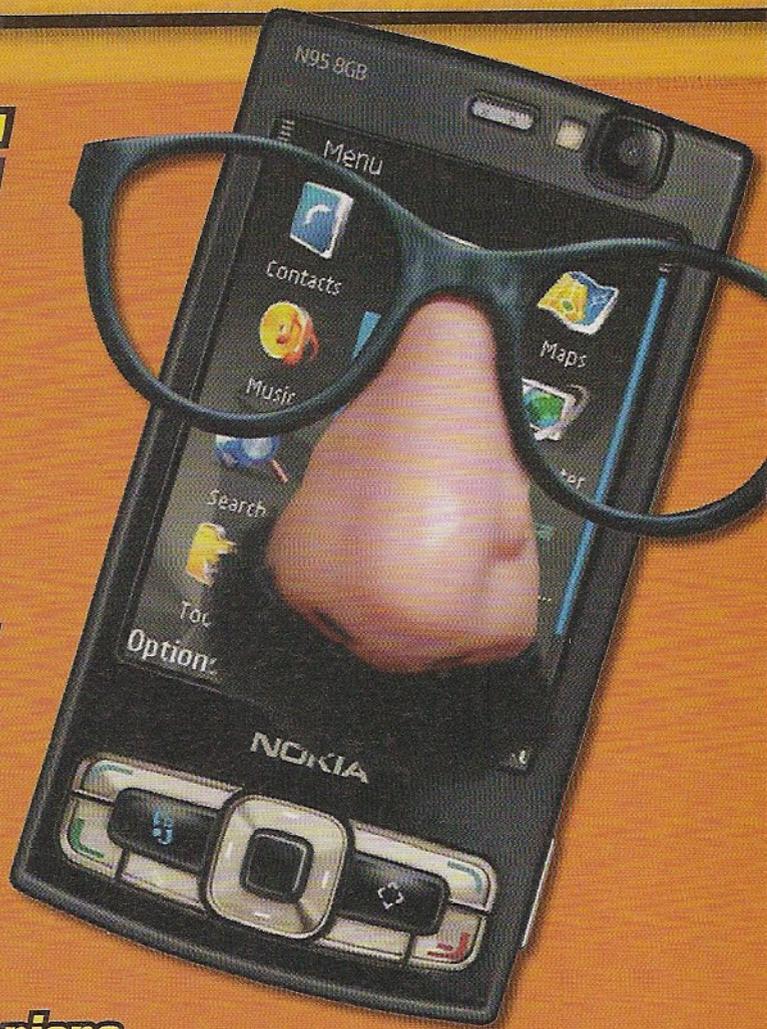
Les plug-in sont l'une des "armes" de WordPress, en permettant d'étendre ses fonctionnalités mais - sans doute aussi pour une question de sécurité et de simplicité de gestion - les développeurs ont décidé de n'en fournir aucun et sur le forum dédié (<http://suprbay.org/forumdisplay.php?f=56>), brokep, fondateur historique de la Baie des pirates, a confirmé cette décision. ■

LE CRIME PAÏE ?

Si l'on en croit un article publié en mai dernier sur [TorrentFreak](http://torrentfreak.com/the-pirate-bay-100-popular-080518/) <http://torrentfreak.com/the-pirate-bay-100-popular-080518/>, avec ses 25 millions de visiteurs mensuels, The Pirate Bay s'est désormais taillé une place parmi les 100 domaines Internet les plus visités. Dans cette liste, qui comprend des noms comme Google, Yahoo!, YouTube, FaceBook et Wikipedia, outre The Pirate Bay, on trouve également Mininova, actuellement sur un podium plus élevé, à la cinquante-deuxième place.

TÉLÉPHONE ESPION

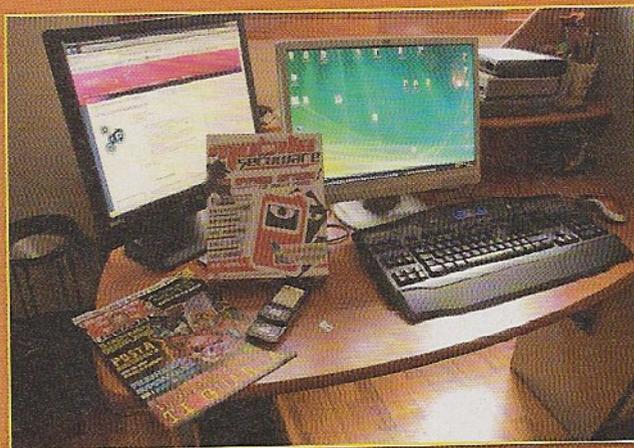
Il ressemble en tous points à un Nokia N95 mais permet en fait de tout savoir de celui qui l'utilise. Hacker Magazine a testé pour vous le plus redoutable des téléphones espions...

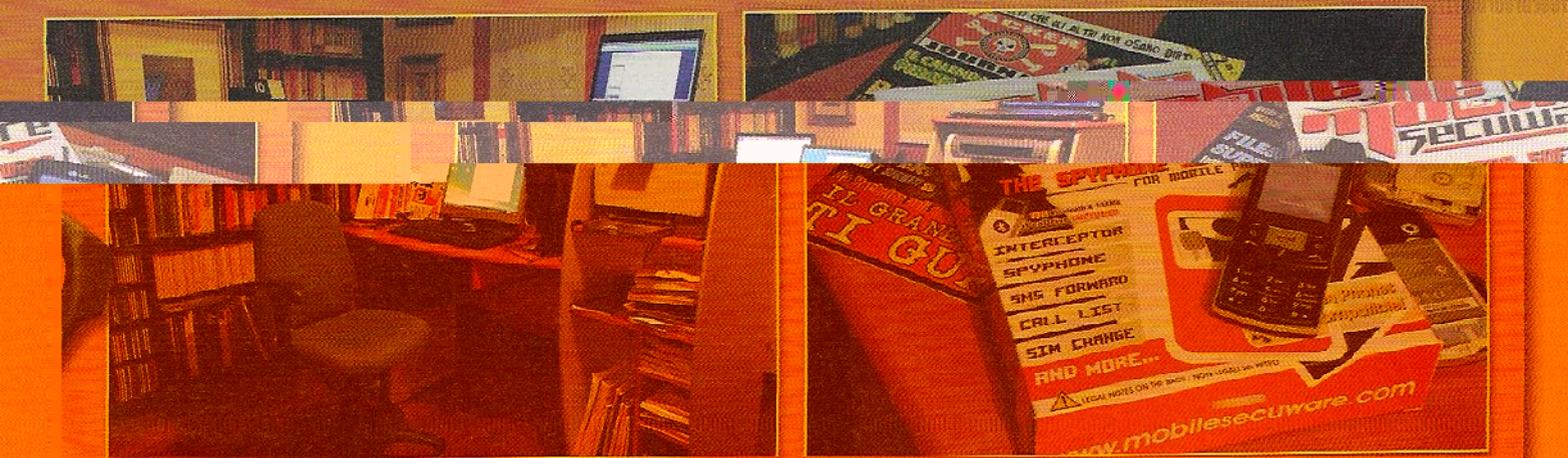


Un a polémique est toujours bonne pour le commerce et The Pirate Bay le sait bien. Il y a quelques mois, la Répression des Fraudes a coïncé 420 personnes qui avaient modifié leur téléphone portable de sorte qu'il puisse espionner fiancées, maris, employés et amants,

en utilisant un programme spécifique. Et ce, en découvrant par la même occasion, les aventures sexuelles d'un couple vivant dans un immeuble de la banlieue de Naples : en fait, le mari était l'amant d'une femme du même immeuble. Rien d'étrange à cela me direz-vous, si ce n'est le fait que le mari de cette dernière était également l'amant de la femme trompée par le premier mari. Complicé, pas vrai ? Et c'est peu dire, puisque la Répression des Fraudes a découvert que nos quatre compères, évidemment méfiants, se contrôlaient mutuellement par le biais de téléphones espions. Sans doute l'un de ceux qu'Hacker Magazine a testé pour

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





matière d'espionnage téléphonique. Bien sûr si vous les achetez pour un usage licite, vous ne commettez aucun délit. Même si ce type d'utilisation est quelque peu ennuyeux : contrôle des nouveau-nés, localisation d'animaux domestiques, surveillance de bruits naturels, utilisations expérimentales et didactiques dans le domaine de la haute fréquence, etc..

:: Faute avouée, à moitié pardonnée

Ceux qui souhaitent disposer d'un téléphone espion complet, peuvent acheter chez NeoCall le Nokia N95 avec Neo-Suite 2K8 OS9 et Neo-Gps. C'est assez cher, 1 399 euros, mais ceux qui ne souhaitent que la Neo-Suite pourront s'en tirer avec 499 euros. Vous pouvez aussi juste acheter certains modules : celui pour intercepter les Sms coûte entre 120 et 195 euros, selon le système d'exploitation Symbian. En ce qui nous concerne, nous avons justement testé le Nokia N95 avec la Neo-Suite 2K8 OS9 et Neo-Gps. Nous l'avons donné à un "cobaye", qui y a inséré sa carte Sim et l'a emmené avec lui au bureau. Nous l'avons tout de même averti qu'il s'agissait d'un téléphone espion et qu'il ne fallait pas trop dire de mal de nous lors de cette petite expérience.

Depuis notre rédaction, en milieu de matinée, nous avons donc commencé à agir. Pour nous dégourdir les doigts et les oreilles, nous avons appelé le téléphone espion avec notre téléphone

"pilote", un mobile normal qui a toutefois été paramétré dans sa configuration initiale de sorte que le Nokia du cobaye le reconnaisse et accepte des commandes très spécifiques. Le téléphone espion a reconnu notre appel et a activé automatiquement la communication : sans vibrer, sans qu'une lumière ne s'allume, sans sonner. Bref, sans donner de signe de vie. Mais en nous permettant d'écouter toutes les conversations dans le rayon d'action du micro du mobile. Au premier essai, pour dire la vérité, l'expérience n'a pas été très concluante vu que le cobaye était une femme qui, en tant que tel, le gardait dans son sac à main. On entendait un peu mais sans vraiment distinguer les mots. Une demi-heure plus tard, le son était nettement plus clair. Quoi de plus normal, puisqu'elle l'avait posé sur son bureau !

:: Espionnage tous azimuts

Après avoir brisé la glace en écoutant quelques commérages de bureau, nous avons envoyé au téléphone espion, via Sms, la commande qui permet d'intercepter les Sms de notre cobaye. Chaque fois qu'elle en recevait ou en envoyait un, ils arrivaient

également sur notre mobile. Pas mal ! Et même, pas mal du tout, vu que selon une récente étude anglaise, la plupart des maris volages envoyant des textos tendres voir plus explicites sont découverts par leur partenaire grâce justement à ce système, en brisant ainsi les ménages. Nous envoyons un autre code via Sms (bien sûr le téléphone témoin ne les montre pas et ne les affiche pas parmi les autres Sms) pour recevoir une notification via Sms de tous les numéros des appels que notre amie a passés et reçus. Si votre fiancée appelle 18 fois le même numéro en l'espace d'une journée, et que ce numéro n'est ni le vôtre ni celui de sa mère, alors votre investissement dans un téléphone espion était-il sans doute justifié. En théorie, nous aurions pu également écouter ses appels, mais sa carte Sim aurait dû être activée pour la conférence (appels à trois). Malheureusement, elle ne l'était pas.. Enfin, une procédure un peu plus difficile nous a permis

d'activer la fonction du software Neo-Gps (199 euros, si vous l'achetez à part) qui permet de savoir dans quelle cellule se trouve le mobile espion, et donc de localiser sa position avec une certaine précision. Rien à dire si ce n'est qu'il s'agit d'un software très intéressant. Dommage qu'il ne soit absolument pas légal de l'utiliser pour espionner les gens. ■



Nulle part à l'abri !

L'évolution de la technologie donne un gros coup de pouce à ceux qui souhaitent pirater les systèmes informatiques.

Il semblerait que les techniciens qui élaborent des projets en général pensent utiliser des composants passifs comme base de leurs circuits en oubliant que ces derniers sont en réalité des systèmes physiques ayant des comportements physiques qui permettent de les comparer à d'autres choses, comme des circuits radio.

D'où la fameuse question : vous avez acheté un excellent pare-feu ? Bien. Gardez-le soigneusement dans un tiroir. Sans doute vous servira-t-il un jour.

Mais pour que cette notion soit bien intégrée, il faut tout d'abord établir une distinction parmi ceux qui, en réalité, tentent de violer les systèmes informatiques.

Première catégorie : les "hackers" qui exploitent les failles des systèmes d'exploitation et du hardware et entrent dans des sites web pour dérober quelques listes de clients ou modifier leur page web. Il y a ensuite ceux qui recherchent des informations dans des systèmes non connectés à Internet, dont les disques sont déposés dans un coffre-fort dès que le travail s'interrompt, et qui vivent dans une pièce dont les fenêtres ne permettent pas d'entrevoir les écrans des systèmes.

Et c'est là qu'entre en jeu le professionnel qui exploite des

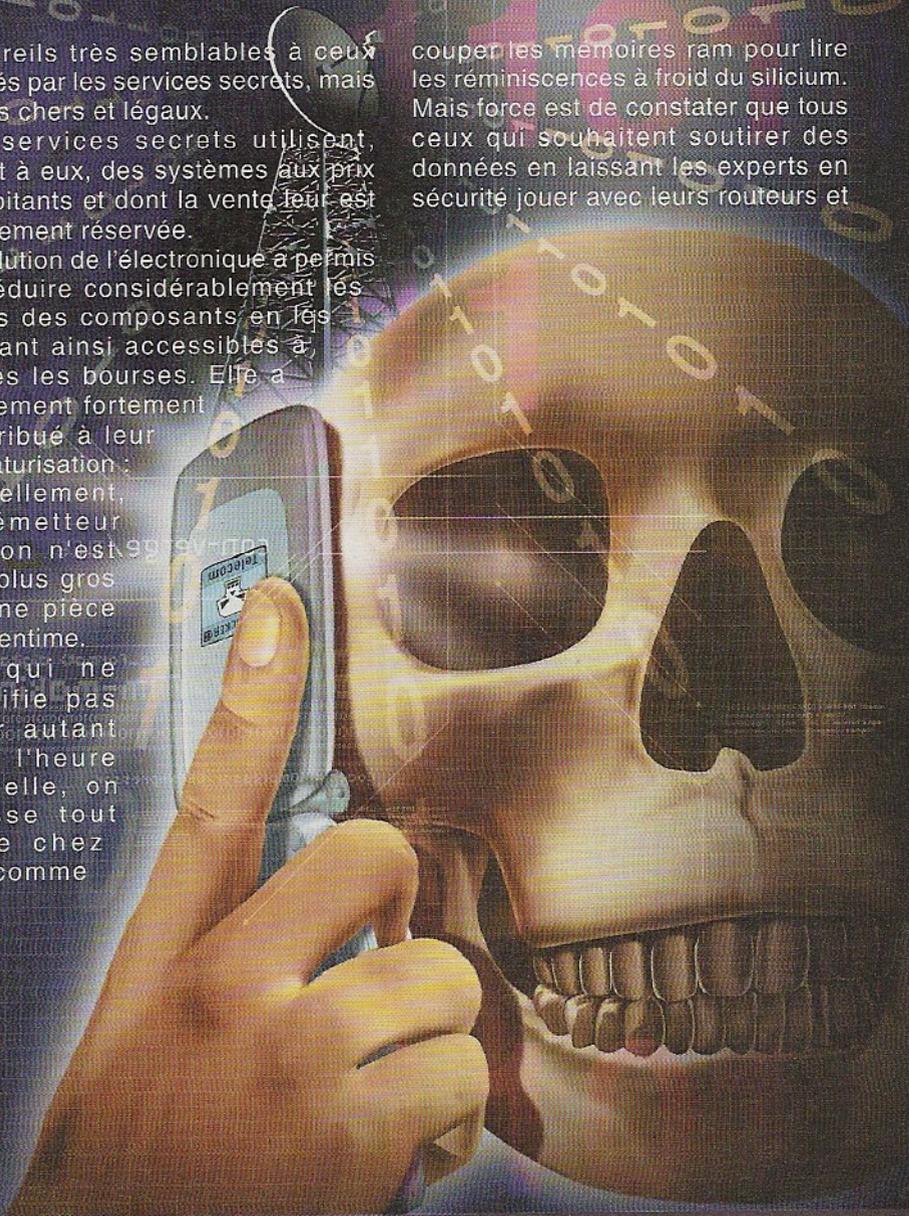
appareils très semblables à ceux utilisés par les services secrets, mais moins chers et légaux.

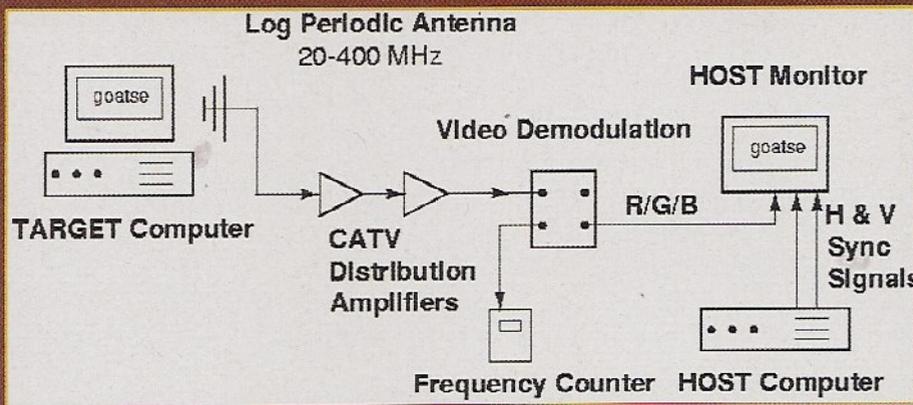
Les services secrets utilisent, quant à eux, des systèmes aux prix exorbitants et dont la vente leur est strictement réservée.

L'évolution de l'électronique a permis de réduire considérablement les coûts des composants en les rendant ainsi accessibles à toutes les bourses. Elle a également fortement contribué à leur miniaturisation : actuellement, un émetteur espion n'est pas plus gros qu'une pièce d'1 centime.

Ce qui ne signifie pas pour autant qu'à l'heure actuelle, on puisse tout faire chez soi comme

couper les mémoires ram pour lire les réminiscences à froid du silicium. Mais force est de constater que tous ceux qui souhaitent soutirer des données en laissant les experts en sécurité jouer avec leurs routeurs et





pare-feu, peuvent le faire en toute quiétude. Il existe différents types d'interceptions, des interceptions de type électromagnétique (radio et téléphones) aux interceptions acoustiques (sons et bruits).

Partons des interceptions électromagnétiques, lesquelles découlent d'un facteur commun à tous les systèmes électroniques.

Ces derniers ont besoin d'une horloge pour fonctionner, appelée clock dans le jargon. Celle-ci est utilisée pour gérer les flux de données sur les circuits logiques du hardware en question.

Si le hardware dont nous parlons est un écran, celui-ci est transformé en émetteur d'images.

Avant d'introduire ce type d'interception utilisé par les hackers professionnels, voici un exemple pour vous montrer son principe physique. Erik Thiele a créé un petit programme qui, en agissant sur les registres de la carte vidéo, crée d'étranges papillotements qui correspondent à

des ondes radio émises par l'écran. Concrètement, pour montrer que les champs électromagnétiques existent, il a pris des MP3 et les a transmis à une petite radio AM/FM en utilisant ces rayonnements, et en obtenant des résultats vraiment impressionnants, laissant souvent bouche bée les experts en informatique.

Nom de ce programme : TEMPEST for ELIZA. Disponible sur le site d'Erik : www.erikykyy.de/tempest

L'interception professionnelle ne nécessite que trois outils :

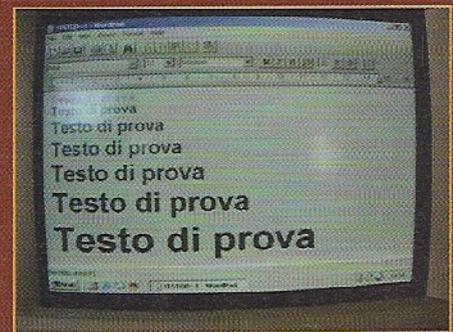
- Une antenne directionnelle à orienter vers les locaux où se trouve l'ordinateur
- Un récepteur d'une bande passante d'au moins 1 GHz
- Deux oscillateurs également réalisés avec deux circuits NE555, lesquels permettent de rechercher les fréquences de synchronisme de l'écran.

Les émissions de l'ordinateur sont généralement produites à des fréquences tournant autour de 60 MHz mais leurs harmoniques grimpent à plus de 3 GHz. C'est pourquoi, si vous disposez d'un analyseur de spectre, vous pouvez remplacer le récepteur par celui-ci. La théorie de départ fut étudiée par Erik Van Eck et ce phénomène fut baptisé TEMPEST (Transmitted Electro-Magnetic Pulse/Energy Standards & Testing).

L'écran des ordinateurs, y compris les LCD, créent ce champ électromagnétique sur des fréquences tournant en général autour de 50 MHz. Chaque onde possède une fréquence de base et

des harmoniques sur les multiples de cette dernière, avec des puissances toujours inférieures.

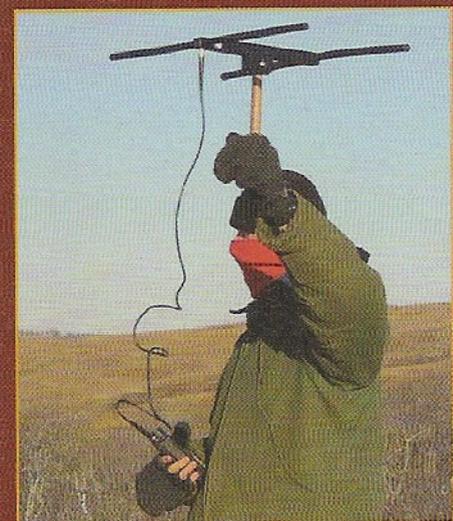
Le problème du récepteur qui doit atteindre des fréquences très élevées est lié à la pollution environnementale des fréquences radio. Même si l'onde porteuse de l'émission de base possède une plus grande puissance par rapport aux harmoniques, sur la



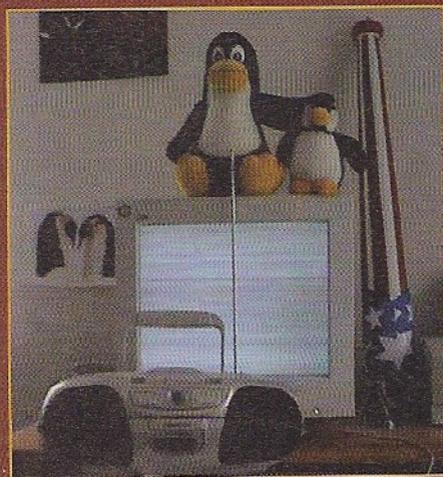
▲ *Ecran d'origine*



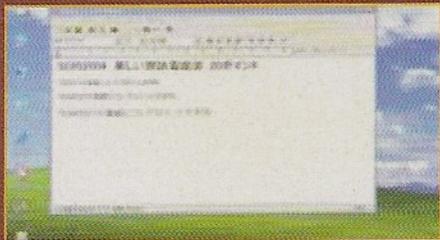
▲ *Ecran intercepté*



▲ *Voici l'utilisation d'une antenne directionnelle*



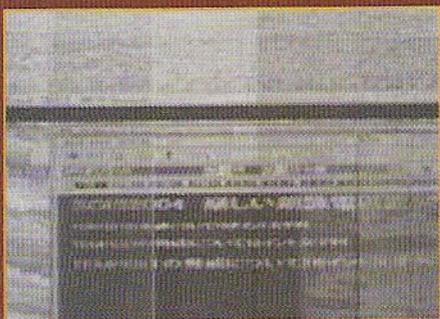
bande 50-70 Mhz, le seuil du bruit radio est très important, et c'est bien là tout le problème. C'est pourquoi en montant en fréquence, les harmoniques baissent de puissance et le bruit radio a lui aussi tendance à disparaître. Ces photos représentent le résultat obtenu à 13 mètres de distance avec un mur au milieu.



▲ *Ecran vers lequel diriger l'antenne*



▲ *Identification des synchronismes*



▲ *Réglage de l'image*

Voici donc quelles sont les phases d'une interception.

Un chercheur Japonais appelé Tanaka a montré comment à l'aide d'un récepteur de radioamateur ordinaire, il pouvait réaliser des interceptions.

L'écrit s'intitule : "A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave."

www.nict.go.jp/publication/shuppan/kihou-journal/journal-vol52no1.2/03-13.pdf

www.nict.go.jp/publication/shuppan/kihou-journal/journal-vol52no1.2/03-13.pdf

Mais, le document le plus complet sur TEMPEST reste celui de Markus Khun, un pdf de 200 pages :

www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf

Ce document approfondit ce sujet dans ses moindres détails, des principes physiques à la théorie électronique jusqu'à l'expérimentation dans ce secteur.

Le problème TEMPEST est toutefois bien plus vaste que ce que l'on pourrait imaginer, dans la mesure où il n'implique pas seulement les écrans des ordinateurs, puisqu'il concerne également les lignes électriques, les fax, les transmissions sérieelles, et bien d'autres choses encore.

Concernant les LCD, lisez ce document :

www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf

Par exemple, les ondes électromagnétiques sont acheminées par les câbles d'alimentation des ordinateurs et, grâce à une analyse faite sur ces derniers, les informations traitées peuvent être reconstituées et affichées. Tanaka en a fourni la preuve...

www2.nict.go.jp/y/y213/tempest/tempest-image6.gif

Les images liées à ce type d'expérience menée auprès de l'Information Security Research Center



National Institute of Information and Communications Technology (NICT) sont disponibles sur le lien suivant :

www2.nict.go.jp/y/y213/english/e-tempest.html

...par le biais de ce récepteur AOR AR8600 MkII.

Vous pouvez l'utiliser à la place de



▲ *Voici un récepteur TEMPEST dont la vente est interdite au public*



▲ *Un récepteur vendu exclusivement aux gouvernements : le Rohde & Schwarz FSET22 qui couvre de quelques HZ à 22 GHz avec une bande passante allant jusqu'à 500 Mhz.*



l'analyseur de spectre, branché à un générateur de signaux, utilisés pour simuler le synchronisme d'écran, et raccordé à un processeur de trame du systemware.

www.bernardotti.it/FrameControl_email.pdf

Et là nous sommes au niveau des services secrets... Avec cet appareillage, vous obtiendrez presque des photos à une distance de plus de 40-50 mètres.

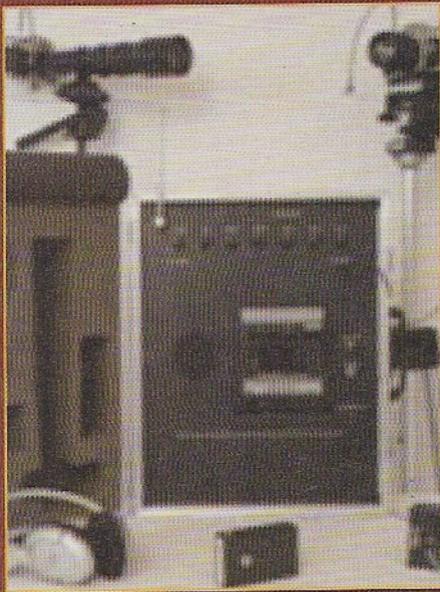
Voici en revanche un lot complet du matériel exclusivement réservé aux gouvernements.

www.bernardotti.it/DSI-1550.pdf

www.bernardotti.it/DSI-1550.pdf

Enfin, pour clôturer le sujet sur tempest, nous vous conseillons de visionner ce petit projet sur :

<http://eckbox.sourceforge.net>

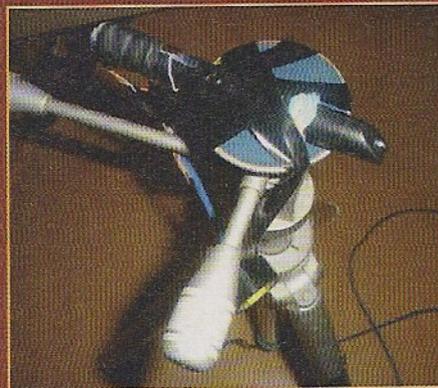


Autre type d'interception : celle liée au bruit des touches tapées. Ce système se base sur le fait que le bruit de chaque touche est légèrement différent. C'est pourquoi un dressage de réseau neuronal lié à un système pour écouter à distance les sons, permet de comprendre ce que la personne est en train de taper.

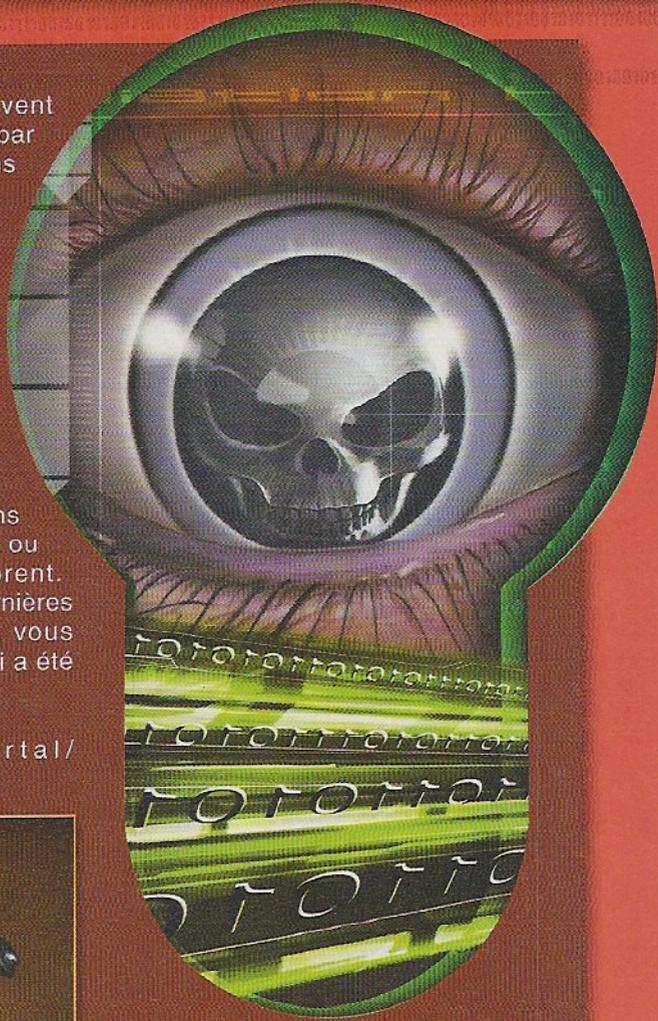
Les touches d'un clavier peuvent révéler beaucoup de choses : par exemple, ce que nous écrivons et même qui nous sommes. Au point qu'une méthode peu connue pour caractériser les personnes qui utilisent un ordinateur spécifique est justement liée à leur façon de taper sur le clavier (testez, par exemple, un programme comme www.divshare.com/download/2523193-3ec !).

Lorsque vous êtes enfermé dans une pièce et que vous parlez ou faites du bruit, les vitres vibrent. Avec un laser pointé sur ces dernières et en analysant la réflexion, vous pourrez donc interpréter ce qui a été dit, à un faible coût (10 €).

www.bernardotti.it/portal/showthread.php?t=2476

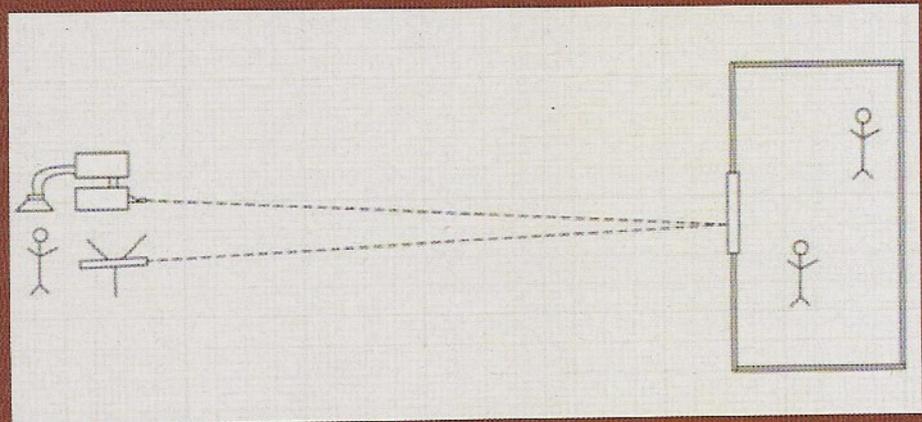


⚠ Branchez la sortie de la photorésistance à un amplificateur, ou à la carte audio du PC



Achetez un pointeur laser et un viseur de fusil à bas prix sur lequel vous monterez une photorésistance.

Branchez-la au PC, elle vous permettra de former un réseau neuronal de façon à interpréter les bruits. ■



⚠ Branchez-la au PC, elle vous permettra de former un réseau neuronal de façon à interpréter les bruits

Être Hacker aujourd'hui

Le temps a passé depuis les premiers exploits du Condor. Les hackers ont aujourd'hui changé de dimension. La preuve avec l'équipe italienne qui a remporté l'édition du "Capture the Flag"



Avouer qu'on était un Hacker avait une saveur toute particulière. Les Hackers étaient les progénitures d'un nouveau courant de pensée, des petits génies de l'informatique, opposants naturels aux règles qui bridait ce monde numérique dirigé par une autorité centrale rigide, froide et calculatrice. Sur ces gros "méchants" dépeints par la presse, seuls quelques-uns étaient devenus des hors-la-loi. A l'âge d'or, le Condor se baladait en toute quiétude dans les serveurs du gouvernement américain et n'avait pas encore été capturé par le FBI. Les Hackers avaient basé leur imaginaire sur des films comme Wargames et les romans de Gibson, ils étaient sur le point d'abandonner les BBS et Packet Radio où il était né, pour migrer en masse vers un Réseau de plus en plus large. Un

monde prometteur s'ouvrait alors à eux, un monde où les utopies semblaient encore réalisables. Les Hackers étaient les porte-drapeau d'un univers immense de connaissances, partagé, et sans restriction aucune. Maintenant que les teenagers de l'époque sont des trentenaires ou des quaranténaires, dont certains ont fondé de florissantes sociétés dans les TIC, on est en droit de se demander qui sont les nouveaux Hackers. Pour le savoir, nous avons décidé d'interviewer un groupe d'entre eux, les Chocolate Makers, qui viennent de remporter une grande compétition internationale.

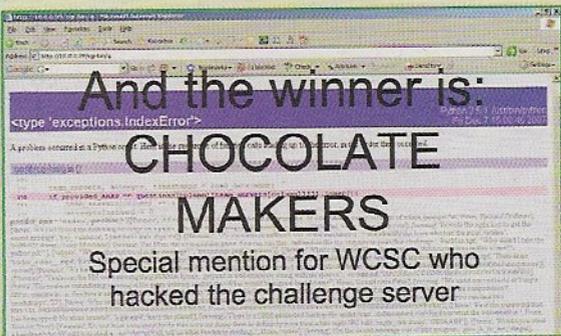
la compétition, et contenant une ou plusieurs vulnérabilités. L'image de la machine virtuelle est ensuite distribuée à l'ensemble des participants. La mission des différentes équipes consiste à étudier les applications développées par les organisateurs, trouver les vulnérabilités, les corriger sur leurs propres machines, et enfin les utiliser pour corrompre les machines des adversaires. Cela fait maintenant plusieurs années que nous participons à ce type de compétition et nous nous sommes quasiment toujours hissés aux premières places... et nous devons dire que cette année nous a plus particulièrement réussi ! Dans ce type de compétition, les groupes les plus forts sont généralement les Européens, et plus particulièrement les Autrichiens et les Allemands.



1) Aujourd'hui, tout le monde ou presque vous connaît, vous avez remporté l'édition 2007 du "Capture the Flag", une compétition mondiale entre groupes de Hackers. Comment se déroule cette compétition ? Comment avez-vous obtenu ce prestigieux titre ? Quel a été le groupe le plus dur à battre et pourquoi ?



2) Pouvez-vous nous raconter l'anecdote qui se cache derrière votre nom, "Chocolate Makers" ?



Les organisateurs de la compétition préparent l'image virtuelle d'un système dans lequel ont été insérées des applications, écrites spécialement pour



La première fois que nous avons participé à une compétition de ce type, nous pensions nous classer parmi les derniers, en faisant ainsi piètre figure, et c'est là que nous avons eu l'idée de ce nom ! (en italien, "fare una figura da cioccolataio" signifie "faire piètre figure").

3) Le terme de Hacker englobe aujourd'hui tout et n'importe quoi. Un terme auquel on a donné trop de sens pour pouvoir être clair et exhaustif. Comment définiriez-vous un Hacker ?

Un "hacker", c'est tout simplement une personne curieuse de savoir pourquoi et comment fonctionnent les choses, et ce dans leurs moindres détails. La plus grande aspiration d'un "hacker", c'est de prouver qu'il est capable de faire des choses que d'autres estiment extrêmement difficiles, voire impossibles. Ce terme ne doit bien évidemment pas être uniquement circonscrit à l'informatique, comme le prouvent les différentes compétitions organisées au sein de manifestations du style DefCon.

4) Comment cohabitent les deux natures qui sommeillent en vous, celle du Hacker et celle du chercheur ? Qu'est-ce qui prend le dessus, le défi ou la soif de connaissances ?

Pour nous, "faire de la recherche", cela signifie essayer de contribuer au progrès d'un secteur scientifique spécifique. Un tel objectif est certainement très proche du concept de "hacking".

5) Autrefois, celui qui devenait Hacker le faisait en suivant un parcours idéologique bien précis, où l'on pourrait parler de "contre-culture". Quelles sont les différences par rapport au passé ? Et qu'est-ce qui différencie un Hacker d'un Expert en sécurité travaillant, par exemple, pour une multinationale ?

Les motivations qui poussent une personne à essayer de devenir un hacker sont probablement les mêmes qu'il y a vingt ans, qu'elles soient idéologiques ou purement "techniques". La principale différence, c'est qu'aujourd'hui, on trouve dans la presse de plus en plus de gens qualifiés, à tort, de "hackers", et qui exploitent certaines failles de sécurité dans le seul but de faire de l'argent. Un expert en sécurité d'une multinationale peut ou non être un hacker, indépendamment du travail pour lequel il est payé.

6) Quels sont, selon vous, les principaux problèmes auxquels devra faire face l'évolution numérique en matière d'éthique informatique ? Quelle doit être la direction à prendre, pour protéger par exemple le droit d'auteur et la confidentialité des données, mais aussi pour combattre la censure des informations sur le Net ?

Nous ne pensons pas que "l'éthique informatique" soit si différente de l'éthique du "monde réel". Les problèmes à affronter sont, grosso modo, les mêmes. La seule différence, c'est qu'ils sont largement amplifiés par le potentiel des outils informatiques.

7) Les journaux créent souvent un vent de panique. Tentons de faire définitivement la lumière sur ce problème : quels sont les risques concrets que court aujourd'hui un "utilisateur informatique lambda" ? Quelques conseils donneriez-vous pour vivre à l'abri des plus grosses menaces ?

Au contraire, je dirais que les journaux ne sont pas assez alarmistes ! Il suffit de voir le peu de considération accordée à la sécurité informatique dans les entreprises. Même un simple utilisateur court de gros risques : vol d'identité, données personnelles ou encore risque d'être infecté par un malware et de faire partie d'un botnet, qui sera loué sur eBay au plus offrant en vue d'actions illégales. Le problème de fond, c'est qu'un ordinateur est un outil extrêmement complexe, que l'on ne devrait pas pouvoir utiliser sans avoir conscience des risques que l'on peut courir... c'est un peu comme vouloir conduire une voiture sans permis !

8) Quelles sont les toutes dernières techniques d'attaque apparues récemment ? Pouvez-vous donner quelques conseils aux Administrateurs systèmes ?

Nous avons assisté ces dernières années à une diffusion à grande échelle des applications web : désormais, presque tous les sites disposent de contenus dynamiques, et la réalisation de ces

applications est bien souvent confiée à des programmeurs dont les compétences en matière de sécurité sont insuffisantes. La plupart des vulnérabilités en circulation concerne donc justement les web application. Plus encore que les gestionnaires de réseau, il serait opportun de sensibiliser les entreprises et autres développeurs quant à l'importance de la formation sur les thèmes liés à la sécurité. Le problème, c'est que dans la plupart des cas, investir dans la sécurité n'apporte pas de gains immédiats et tangibles.



BOTNET : bientôt tous des zombies ?

Dans le folklore haïtien, un zombie est un mort ressuscité par un sorcier pour faire son sale boulot, un peu comme une marionnette. Mais ne riez pas trop vite, car tel pourrait être le destin de votre PC dans un réseau botnet...

Parmi les mille et une stratégies imaginées par les hackers et autres pirates pour prouver leur habileté technique et se faire de l'argent facile, les réseaux botnet décrochent sans aucun doute la palme d'or en termes d'ambition et de puissance. En effet, si l'on peut comparer les virus, chevaux de troie et vers à des "criminels" indépendants du monde informatique, les réseaux botnet, eux, s'assimilent davantage à des réseaux mafieux voire au terrorisme organisé.

== Virus contre bot

Un botnet est un réseau d'ordinateurs infectés par un bot, terme anglais qui n'est autre que l'abréviation du mot robot. Le malware traditionnel et les bot ont de nombreux points communs. Tous deux se diffusent

en s'installant sur les ordinateurs d'utilisateurs lambdas connectés à Internet. Tous deux peuvent exploiter différentes méthodes pour s'infiltrer sur vos machines : téléchargement de site ftp ou sur Internet, envoi à travers file torrent, pièces jointes d'e-mails, messagerie instantanée comme MSN ou ICQ... Mais si d'un côté, virus et autres programmes du même type agissent individuellement et selon une programmation bien définie, toujours égale à elle-même, de l'autre, les bot sont de petits programmes indépendants qui agissent ensemble sous le contrôle d'un "esprit" unique, à savoir la personne qui contrôle le réseau botnet. Cette personne, le botmaster ou botherder, disposera sur un serveur distant du programme de contrôle, appelé dans le jargon Command and Control ou C&C. Les bot envahissent alors vos ordinateurs et attendent que leur coordinateur lance une action combinée

à travers le C&C : concrètement, ils se comportent comme les cellules inactives d'un réseau terroriste.

== Une infinité de possibilités

L'importance des botnet dans l'univers du piratage informatique est souvent sous-évaluée. Premièrement, ces petits programmes parviennent souvent à s'infiltrer, même dans les systèmes les mieux protégés contre virus et autres malware. Et deuxièmement, ils sont capables d'organiser des attaques combinées à grande échelle. Ainsi, la plupart de la "junk mail", ces courriers indésirables qui inondent tous les ordinateurs du monde entier, est gérée par botnet. Les milliers (voire millions) de messages sont en effet envoyés depuis les ordinateurs d'utilisateurs



lambdas, sous le contrôle de botmasters largement rétribués pour leurs services. Mais ce type d'exploitation de ressources n'est pas le seul risque auquel s'expose votre ordinateur. En effet, les bot peuvent aussi garder sous contrôle votre clavier pour vous dérober vos mots de passe d'accès aux sites, votre numéro de carte bancaire ou encore d'autres informations sensibles pour vous voler votre identité et votre argent.

:: Techno-extorsions

Autre grand cheval de bataille des bot : les attaques DDoS ou Distributed Denial of Service (littéralement "Déni de service"). Ce type d'attaque va inonder de demandes un système informatique fournissant un service, comme un site Internet, pour le pousser au-delà de ses performances maximales et donc le bloquer. Si le pirate utilisait son propre réseau d'ordinateurs pour lancer une telle attaque, il serait alors facile de remonter jusqu'à lui ! Il est donc bien plus pratique et efficace de diffuser des bot en passant par l'une des méthodes dont nous venons de parler. Lorsqu'un nombre suffisant de machines est infecté (ou encore à l'occasion d'un événement particulier ou à une certaine date), le botmaster ordonne alors à tous les ordinateurs sous son contrôle (appelés zombies, dans le jargon informatique) d'envoyer les demandes de services à la cible. Compte tenu du nombre d'ordinateurs possédant aujourd'hui une connexion haut débit et de leurs systèmes de protection limités, le phénomène des botnet utilisés pour lancer des attaques DDoS s'amplifie donc de plus

en plus et commence à prendre des proportions alarmantes. L'objectif ? L'extorsion de fonds dans la plupart des cas. Les pirates vont bloquer, par exemple, un site commercial et demander ensuite une "rançon" pour son retour à la normale. Dans d'autres cas, les attaques DDoS sont utilisées comme moyen pour paralyser la concurrence ou encore pour manipuler des événements politiques, en bloquant par exemple le site d'un candidat le jour des élections.

:: Menus larcins et escroqueries à grande échelle

Les botnet peuvent aussi être utilisés pour fausser les retours publicitaires d'un site Internet. Par exemple, si votre site commercial contient des bandeaux publicitaires "pay per click" (celui qui achète la publicité vous paie en fonction du nombre de personnes qui ont cliqué sur sa fenêtre ou banner) ou "pay per install" (le client offre un programme et vous paie en fonction du nombre de personnes qui l'installent), vous pouvez soudoyer un botmaster pour obtenir des milliers de clics et autres installations d'utilisateurs qui, en réalité, n'auront même jamais vu le fameux message publicitaire. Mais bien souvent, c'est un concurrent véreux qui utilise les services d'un botnet pour inonder de clics ou de téléchargements la société adverse et ruiner ainsi sa réputation auprès de ses clients. Alors, véritable paranoïa ? Non, car c'est exactement ce qui est arrivé à Google il y a quelques années : accusé de négligence après que des personnes malintentionnées ont violé la fonctionnalité de

ses bandeaux publicitaires, le moteur de recherche a décidé de mettre fin au procès en payant 90 millions de dollars.

:: La contagion se répand

Outre le fait de pouvoir effectuer de nombreuses tâches, les botnet ont aussi la capacité de s'étendre et de s'actualiser. Les botmasters peuvent insérer sur l'ensemble du réseau leurs dernières trouvailles, tout en utilisant les bot pour chercher les ordinateurs les plus vulnérables sur lesquels s'installer. En outre, un réseau botnet devient de plus en plus puissant au fur et à mesure qu'il grandit, avec en conséquence une capacité d'extension de plus en plus importante. Alors, quand un zombie réveille l'autre...

:: Carrières de pirate

L'un des aspects les plus préoccupants du phénomène des bot est qu'ils parviennent même à s'infiltrer dans des systèmes apparemment blindés. Ainsi, même des réseaux professionnels

LA COMMUNAUTÉ DU MALWARE

Certains développeurs de botnet sont même allés jusqu'à adopter la stratégie du code open source. Ces pirates rendent public le code de leurs programmes, autour desquels se créent de véritables communautés prêtes non seulement à tester le produit et fournir des conseils quant à d'éventuelles limites ou défauts, mais aussi à collaborer activement à son amélioration en ajoutant des parties de code. Souvent, les membres de la communauté facilitent aussi la diffusion internationale des bot en les traduisant dans leur propre langue. Bien évidemment, les bot qui peuvent s'appuyer sur une large communauté sont encore plus difficiles à localiser et bloquer dans la mesure où ils jouissent de nombreuses variantes : un véritable défi pour ceux qui tentent de créer des stratégies de défense !



bien défendus contre différents types de virus et autres attaques informatiques sont victimes d'attaques de bot et botnet. Le fait est que cette forme de piratage se développe sur un marché très florissant, avec une clientèle étoffée qui se donne les moyens d'investir. Une forme d'attaque hautement spécialisée, donc, non seulement d'un point de vue technique mais aussi organisationnel. Les programmeurs à l'origine des bot sont bien souvent de petits génies de l'informatique qui exploitent des techniques avant-gardistes, mêmes pour les standards industriels. L'environnement est en outre très concurrentiel et ces professionnels du malware "font la course" pour produire les bot les plus efficaces ou les plus discrets. Les techniques utilisées pour éviter que le serveur de gestion du C&C ne soit repéré et bloqué sont souvent très élaborées. On peut ainsi trouver plusieurs serveurs centraux prenant le contrôle en cycle, chacun pendant quelques minutes consécutives. Un C&C principal peut aussi déléguer la gestion du réseau à plusieurs C&C secondaires sur des serveurs différents. Bref, une véritable hiérarchie, similaire à celle d'une organisation militaire.

:: Un marché en forte croissance

Autant de professionnalisme serait pur gaspillage et difficilement finançable s'il n'existait pas un marché du botnet. En réalité, leur flexibilité et leur puissance peuvent s'avérer très utiles pour différents "clients" :

outre bien évidemment les hackers et spammers, on trouve aussi le crime organisé, les groupes terroristes, les extrémistes politiques, les professionnels de l'espionnage industriel ou quiconque aurait un intérêt, par exemple, à bloquer un service basé sur Internet. Le marché est tellement organisé qu'il existe même des médiateurs professionnels faisant office d'interface entre les techniciens et leurs clients. Les transactions s'effectuent généralement via chat ou par e-mail. Avec les bons contacts, il est ainsi possible de "louer" un botnet pour lancer une attaque de son choix à travers des dizaines voire des centaines de milliers d'ordinateurs. Aux Etats-Unis, certaines affaires ont déjà été portées devant la justice contre des "distributeurs" de services de botnet avec un niveau de professionnalisme tout simplement bluffant, à même de fournir à leurs clients des produits éprouvés et un service d'assistance technique.

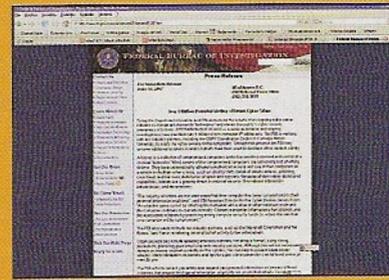
:: Les contre-mesures

Les fournisseurs de service Internet bloquent généralement les attaques DDoS avec une méthode aussi efficace que douloureuse pour leurs clients. Lorsqu'ils se rendent compte qu'une URL donnée fait l'objet d'une attaque, ils déroutent son trafic sur une adresse désactivée, en faisant aussi perdre à leur clients les messages légitimes. S'ils peuvent donc proposer une défense contre les attaques DDoS, même si celle-ci a ses limites, leurs ressources pour combattre les autres formes de nuisance et fraudes liées aux bot restent sombres et modestes.

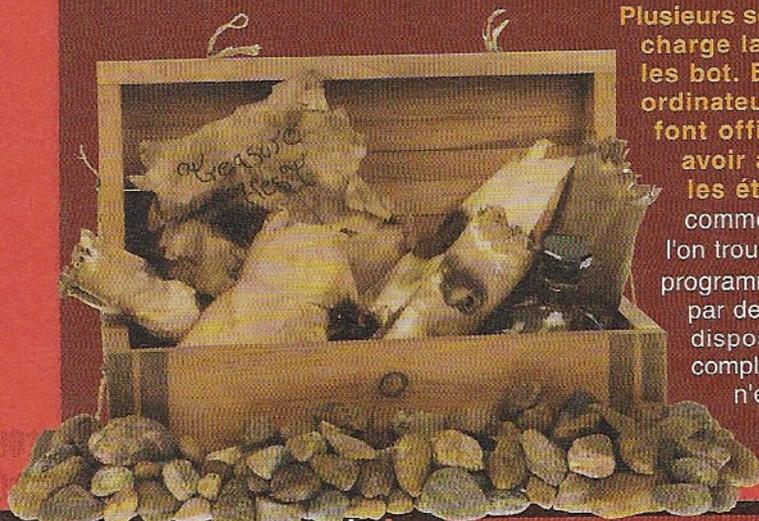
Plusieurs sociétés prennent en charge la protection contre les bot. Elles installent des ordinateurs vulnérables qui font office d'appât. Après avoir attiré les bot, elles les étudient pour trouver comment les désactiver. Si l'on trouve sur le marché des programmes antibot proposés par des sociétés de renom, disposer d'une protection complète pour son système n'est pas chose facile, dans la mesure où

FBI SUR LE PIED DE GUERRE

Aux Etats-Unis, les forces de l'ordre ont bien conscience du phénomène des botnet et des risques qu'il engendre. Le 13 juin de l'année dernière, le FBI a publié les résultats de la première partie de l'opération BOT ROAST, une enquête menée à l'échelle nationale, toujours en cours, et qui, à l'heure du communiqué, avait identifié plus de 1 million d'adresses IP d'ordinateurs utilisés comme zombies. Le FBI collabore avec plusieurs grosses sociétés dans la lutte contre les fraudes informatiques et les botnet, mais sur ce point, la situation juridique reste floue, même aux USA. Concrètement, seuls font l'objet d'une enquête les cas d'escroqueries à grande échelle ou ayant causé de lourds préjudices à de grosses sociétés. Le reste de la population est laissé pour compte et ne doit compter que sur lui-même pour assurer sa défense. Et même lorsque le gouvernement décide d'intervenir, ces fraudes étant organisées à travers des milliers d'ordinateurs dans différents pays, les affaires deviennent alors très difficiles à gérer dans la mesure où elles prennent une envergure internationale et impliquent donc des problèmes de juridiction.



de nouveaux bot apparaissent chaque jour et que les organisations qui les gèrent sont de plus en plus riches et préparées. Allons-nous donc tous devenir des zombies ? Non bien sûr ! Il convient toutefois de se doter d'un bon antibot, de mettre à jour en permanence les programmes utilisés sur son ordinateur pour limiter au maximum le nombre de failles et vulnérabilités et... de toujours garder un œil ouvert ! ■



Free stickers

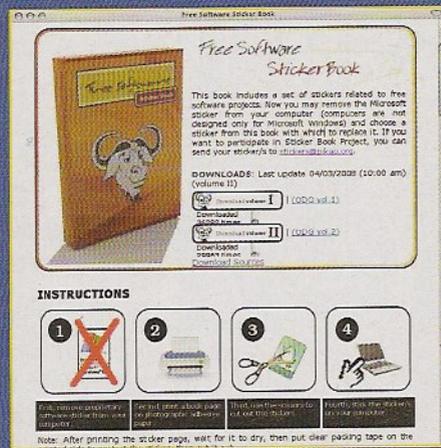
Libérez votre ordinateur grâce aux autocollants !

Placarder des autocollants partout, une manie typiquement américaine mais qui touche également la France depuis quelques années : plaques d'immatriculation, pare-chocs, vitres, valises, sacs et... ordinateurs, rien n'y échappe. Ostentatoires certes, ces stickers sont également utilisés comme outil promotionnel. Même les unités centrales et surtout les portables deviennent parfois des "toiles" sur lesquelles apposer des marques que nous apprécions ou des messages que nous partageons, en retirant ceux qui nous plaisent le moins. Après avoir évincé les logos de Windows ou du fabricant du processeur, les amateurs de Linux ou des logiciels libres FOSS peuvent se mettre à décorer librement leurs postes avec la marque du pingouin et du GNU. Vous trouverez ci-dessous quelques ressources dans lesquelles puiser.

:: Le livre des stickers

L'initiative la plus complète se nomme **Free Software Sticker Book** (<http://www.openstickers.com/>). Ce site rassemble en effet une énorme quantité d'images dans deux fichiers PDF à télécharger, imprimer sur papier adhésif, découper et utiliser. Et parler de "quantité énorme", c'est peu dire ! Les deux PDF proposent respectivement 95 et 72 pages remplies de dessins, logos, couvertures de CD et illustrations couvrant l'ensemble du savoir informatique alternatif : du pingouin Tux au symbole des hackers en passant par aMule et apt-get sans oublier les symboles des principales distributions Linux.

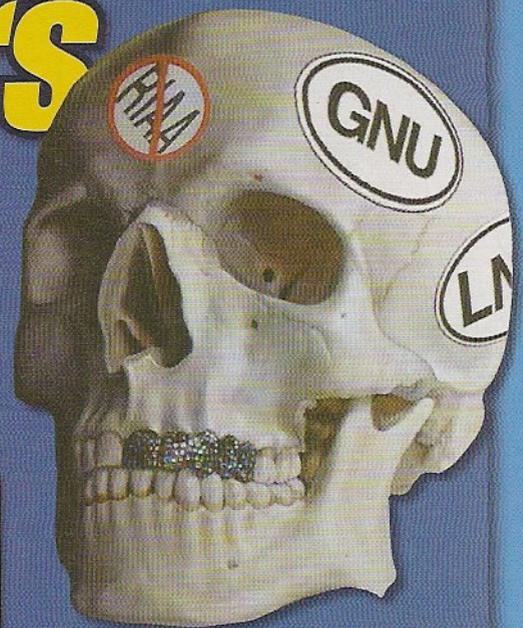
:: Gratuits, ouverts et libres



Free Software Sticker Book va dans le sens des initiatives et softwares qu'il sponsorise. Quiconque peut donc y participer en envoyant ses propositions par e-mail et télécharger le produit fini ainsi que les sources avec des logos connus et moins connus au format vectoriel SVG et XCF (celui de Gimp) pour les modifier et même les vendre.

:: Vista ? Non, merci !

Autre collection de logos à imprimer : celle appelée "Vista



Incapable". Tout a commencé par un avatar sur Internet. L'utilisateur avait choisi le logo qui caractérise les ordinateurs à même d'exécuter Windows Vista mais conseillait (avec pragmatisme ?) de rester sur XP. La réponse d'un ubuntuien ne se fit pas attendre (<http://www.madman2k.net/article/69>). De là a germé l'idée de continuer sur cette vague à travers un forum (<http://forums.raiden.net/viewtopic.php?t=9699>), proposant des créations glorifiant généralement Linux et plus particulièrement PCLinux.



ArchLinux et même FreeBSD, en donnant également des informations sur les caractères utilisés.

Vous trouverez le résultat final de ces créations sur le site web www.vistaincapable.com qui héberge également une autre série à imprimer et coller, appelée "Liberated by (Linux Distribution)".

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

eMule

eMule & CO



N°1

LE MAGAZINE DES LOISIRS NUMÉRIQUES

PRIX
MALIN

2 €

TÉLÉCHARGER

sur

eMule,

LPHANT, EDONKEY, ETC.

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

→ PARAMÉTRER

LiveBox,
NeufBox,
FreeBox,
HighID
pour tous

→ COMPRENDRE

CHOISIR &
INTÉGRER LA
**BONNE LISTE
DE SERVEURS**



→ ASTUCE

100 % ANONYME :
MASQUER
son identité

NOUVEAU
N°1

LE MATCH

Lphant :
Plus fort
que la Mule ?



> À DÉCOUVRIR AUSSI...

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

eMule & BitTorrent
en un seul logiciel !

WLF
PUBLISHING

Soutenez nous, achetez le magazine !