

TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

0% DE PUBLICITE
LISTE DES ARTICLES
2.00 €

www.hackernewmag.it
HACKER
news
Magazine

SEX & VIRUS

Notre voyage au **PAYS DES SOVIETS**
au coeur des **CRÉATEURS DE VIRUS**

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

COMMENT **GOOGLE**

A ÉTÉ **BERNÉ**

L'interview **EXCLUSIVE**

CARTES DE
CRÉDIT'S

les **CARTES CLONES** débarquent
et **MENACENT** tout !

LES EXPERTS
~~**MIAMI**~~ **HACKERS**

Analysez les **PHOTOS** et **VIDÉOS**
comme les experts du **FBI**

ESPIONNAGE

toutes les **TECHNIQUES** pour **ÉCOUTER SANS ÊTRE VU**



Les camarades de la rédaction européenne :

Gregory, Fred, Damien Bancal,
One4Bus, Max, G. Tronconi,
K2der, Sylvain, Silvio De Pecher,
Contents by MDR.

Traduction et adaptation :

Laurent et Sylvie Arsenau

Couverture:

Daniele Festa

Éditeur :

WLF Publishing SRL
Via Donatello 71
00196 Roma

Imprimeur : Roto 2000.

Via Leonardo da Vinci 18/20
Casarile (MI) Italy

Distribution:

MLP - 55 bd de la Noirée
ZA de Chesnes
38070 St Quentin Fallavier

Directeur de la publication :

Teresa Carsaniga

Dépôt légal : à parution

ISSN : en cours

Copyright WLF Publishing

Les droits sont réservés et protégés

Pour la version imprimée.

La rédaction n'est pas responsable des
textes, documents, photos, dessins qui lui
sont communiqués et n'engagent que la
responsabilité de leurs auteurs.

Sauf accord particulier et publiés ou non, ils
ne sont pas renvoyés.

Les indications de prix et d'adresses
sont de l'information fournie sans
aucun but publicitaire.

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

Jeux olympiques : l'important c'est de censurer

*"La liberté n'offre qu'une chance d'être meilleur, la servitude n'est
que la certitude de devenir pire."
Albert Camus (1913-1960)*

*Je ne sais pas pour vous, mais moi je suis vraiment écœuré, et si ce n'était pas par
respect pour nos lecteurs, cette page serait remplie d'insultes et de grossièretés tant
mon indignation est grande !!!*

*Tout ce qui se passe en Chine à l'approche des Jeux olympiques est totalement
scandaleux !*

*Que le Tibet soit un pays brimé et que la Chine bafoue
les droits de l'homme, tant au Tibet qu'en Chine, n'a
rien d'un scoop ! Et pour ceux qui auraient encore
des doutes, qu'ils prêtent l'oreille à toutes ces
dénonciations des organisations de défense
des droits de l'homme... Des faits qui, à
eux seuls, auraient dû convaincre le Comité
olympique de ne pas choisir ce pays
comme hôte d'une manifestation cen-
sée être à elle seule un hymne à la libe-
rté et à la paix.*

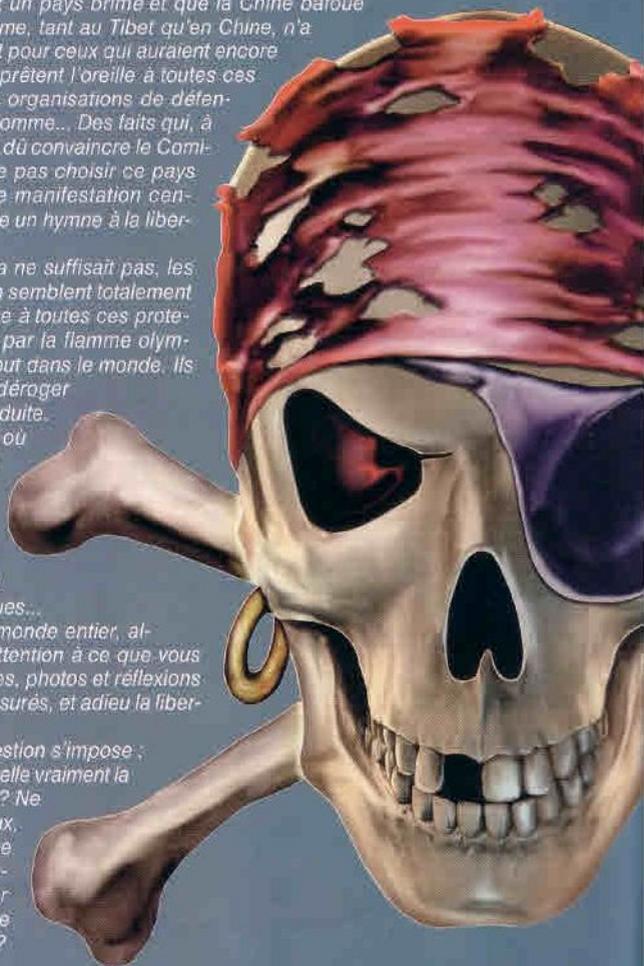
*Et comme si cela ne suffisait pas, les
dinges de Pékin semblent totalement
imperturbables face à toutes ces pro-
testations suscitées par la flamme olym-
pique un peu partout dans le monde. Ils
poursuivent sans déroger
à leur ligne de conduite.*

*D'ailleurs, à l'heure où
nous écrivons, le
ministre de la cul-
ture chinois a mê-
me déclaré qu'In-
ternet risquerait
d'être censuré lors
des Jeux Olympiques...*

*Journalistes du monde entier, al-
lez-y donc, mais attention à ce que vous
dites car vos articles, photos et réflexions
pourraient être censurés, et adieu la libe-
rté d'expression...*

Dès lors une question s'impose :

*Cette partie vaut-elle vraiment la
peine d'être jouée ? Ne
vaudrait-il pas mieux,
pour rester en phase
avec l'esprit olym-
pique, s'éclipser
et renvoyer tout le
monde... chez soi ?*



La NSA comme vous ne l'avez jamais encore regardée

Si on vous parle du 9800 Savage Road ? Les plus géographes d'entre vous se souviendront qu'il s'agit de l'adresse de la NSA, la National Security Agency. Aujourd'hui, avec Internet, il est possible de regarder certains secrets des espions de l'Oncle Sam en quelques clics de souris

Les militaires américains ont pris le taureau par les cornes. Début mars, ils faisaient interdire à des employés de Google de filmer une base militaire Texane. Les employés ne faisaient aucunement de l'espionnage, juste une préparation à une mise à jour de Google Earth, le map monde numérique du géant de l'Internet américain. «Nous avons reçu un rapport nous informant que Google avait collecté une imagerie détaillée et des vues à 360 degrés d'une base au Texas, a expliqué un porte-parole du commandement des forces armées en Amérique du Nord, Gary Ross, Nous n'avons pas de problème vis-à-vis de Google Earth, c'est un instrument très utile, mais quand ils sont sur une base, ils prennent des images détaillées des points de contrôle, des bâtiments du quartier-général, des installations de sécurité... Et cela pose un risque opérationnel». Il est vrai que les détails sont très précis... chez un concurrent de Google Map, la carte satellite mise en place par Microsoft (Live Maps). La dernière mise à jour en date montre des détails de la NSA, la National Security Agency, les grandes oreilles des Services Secrets Américains.

Il est possible de survoler et de se rapprocher de très près de détails qu'un espion n'aurait pu rêver atteindre il y a encore 10 ans, Microsoft n'a pas gommé les détails comme l'a imposé la NSA à Google.

:: Les e-maps, auxiliaires à espions ?

Début mars, des manifestants britanniques parvenaient à grimper sur le toit du Parlement de Londres afin de manifester au sujet de l'extension de l'aéroport de Heathrow. Ils vont réussir ce coup impressionnant en exploitant les détails des toits proposés par Google Map. Allez, une petite dernière pour la route. Saviez-vous que les numéros de téléphones et les identités (très certainement fausses) de personnes travaillant au 9800 Savage Road sont lisibles sur Internet et cela grâce à un annuaire inversé. Tapez, par exemple, le numéro de téléphone (301) 688-0400 dans le moteur américain Switch Bord. De quoi rendre dingue ceux qui sont chargés de la sécurité de la NSA !

D'AUTRES PHOTOS...

D'autres photos de la NSA
<http://cryptome.org/nsa08/nsa08-birdseye.htm>

Les images de la NSA et de lieux secrets via les Maps Google et Live
<http://maps.google.com/maps?f=q&hl=en&geocode=&q=eglin+air+force+base,fl&ie=UTF8&ll=30.573134,-86.214765&spn=0.007916,0.016994&t=k&z=17>

<http://maps.live.com/default.aspx?v=2&cp=qh7rc8m25mn&style=o&lvl=2&tilt=-90&dir=0&alt=-1000&scene=9559611&encType=1>

<http://maps.live.com/default.aspx?v=2&cp=39.103615~-76.764929&style=a&lvl=16&tilt=-90&dir=0&alt=-1000&scene=9559611>

Les pseudos et vraies identités des agents de la NSA
<http://switchboard.intelius.com/reports.php?qi=1&ReportType=33>



PIÈGE SUR INTERNET

Un groupe de pirates a infiltré, en avril, plusieurs dizaines de milliers de sites web afin d'y cacher un iframe, qui permettait d'installer un code malicieux dans les ordinateurs des visiteurs des dits sites web piégés. Le moteur de recherche Google (www.google.fr/search?hl=fr&q=nihaorr1.com+%amp;meta=) montre que les sites attaqués. Toutes les pages renvoyaient vers un espace basé en Chine. De son côté Sophos annonce que ce type d'attaque était devenue un véritable fléau. Le premier trimestre 2008 aura permis d'identifier 15,000 pages web piégées par jour. En 2007, Sophos indique avoir bloqué une page piratée toutes les 14 secondes, en 2008, une page bloquée toutes les 5 secondes. Les USA seraient devenus le principal hôte des pages piégées. En 2007, l'Amérique n'accueillait qu'un tiers des sites compromis.

4 FRANÇAIS ARRÊTÉS

La brigade financière de Montpellier a stoppé 4 jeunes pirates informatiques ayant blanchi de l'argent après des attaques de type hameçonnage, du phishing, avec la complicité d'un pirate Tunisien. Février 2008, une commission rogatoire était ouverte pour découvrir qui se cachait derrière plusieurs escroqueries visant des clients de la société de paiement en ligne Paypal, filiale d'eBay. Une jeune étudiant en BTS de Montpellier était arrêté dans une poste alors qu'il tentait d'envoyer un colis en Tunisie. Les policiers vont saisir à son domicile du matériel hi-fi et des bordereaux d'envoi de colis en Tunisie. 4 mois plus tard, le premier pirate et 3 complices se retrouvent avec des plaintes allant

de l'escroquerie en bande organisée et recel d'escroquerie en bande organisée. Un 5ème homme dans cette histoire est apparu. La tête pensante de cette escroquerie. Connu sous le pseudonyme de Xtazy (Walid Y., 18 ans), un Tunisien. Le pirate exploitait les informations laissées par les membres de son forum pour tenter de rentrer dans les comptes Paypal de ces derniers. Une commission rogatoire internationale a été lancée.



PRISON POUR DES DÉTECTIVES PIRATES

En 2005, des officines de détectives privées se retrouvaient stoppées par les services secrets israéliens. Il avait été découvert qu'elles avaient utilisé des chevaux de Troie (Troïen) pour espionner des entreprises. Durant 18 mois, les détectives privés ont surveillé les concurrents de sociétés comme YES satellite TV, Bezeq

Telephone Communications et Cellcom. Un couple était à l'origine des spywares. Ruth Brier-Hæphrati, 28 ans, a pris quatre ans de prison ferme pour la vente des troïens. Son mari, Michaël Hæphrati, 44 ans, a été condamné à deux ans de prison pour la créations des «outils» espions.

Ils commercialisaient leurs troïen 350 euros pièce. Quatre détectives de la société d'investigation, Modi'in Ezrahi, ont été condamnés à 19 et 18 mois de prison.

JACKY CHAN SE PREND UNE RACLÉE PAR LES PIRATES

Visage sombre, pas un sourire, les mains en train de cadrer un plan sur le spectateur. L'affiche mise en place par la MPA-I, l'association de lutte contre le piratage de film sur Internet, profite de la notoriété de l'acteur Chinois Jacky Chan pour tenter de faire passer son message. Mission, parler du piratage de film. Titre "Protect movies, say No to piracy".



HOT NEWS

FAUX VENDEUR EBAY ARRÊTÉ

Un pirate informatique, de la grande famille des escrocs de types scammeurs, est passé devant la justice Britannique de la ville de Burnley pour avoir piégé au moins 1,600 clients du site de vente aux enchères américain eBay. Jonathan Hartley, 26 ans, fait face aux chefs d'accusations de blanchiment d'argent, de vente de contrefaçons et fraude. Il est accusé d'avoir utilisé un certain nombre de fausses identités (faux mails, faux comptes eBay...) pour réaliser des ventes fantôme. La plupart du temps, il ne livrait pas les produits, et pour cause, il ne possédait pas ce qu'il annonçait vouloir commercialiser. Un grand classique qui ne reste plus impuni. Du moins quand la justice réussit à mettre la main sur ce type d'escroc.

VOLER LES DONNÉES FACEBOOK

La chaîne britannique BBC a proposé une démonstration qui démontrait que Facebook était un véritable danger pour la vie privée. La méthode était simple comme tout. D'abord ouvrir un compte Facebook. Ensuite écrire une petite application, un widget, que les autres membres pouvaient télécharger. Mission de ce gadget, intercepter les noms, les adresses postales, les courriels, les noms des employeurs, de l'ensemble des amis, des amis, des amis, des amis inscrits Facebook. Il n'était pas utile d'enregistrer ce widget pour voir ses informations aspirées. Il suffisait d'être un «pôte» d'une personne piégée. <http://news.bbc.co.uk/1/hi/technology/7376738.stm>

UN COFFEE AVEC LES POLICES DU MONDE

Les policiers du monde entier, dont des Français, le FBI ou encore l'armée, sont invités par Microsoft afin de découvrir et utiliser, dans les locaux de Microsoft à Redmond, l'outil COFFEE (Computer Online Forensic Evidence Extractor). Ce programme regroupe en fait plusieurs logiciels : crackeurs de mot de passe, regroupement d'informations retrouvées sur le disque dur, aspiration de la ram, cracker le chiffrement Bitlocker de Vista, ... Le matos est simple, une clé USB et COFFEE capable de trouver différentes données cachées sur un disque dur. Un programme aux 150 commandes qui permettent de retrouver toutes données liées à une affaire en un temps record. Un peu plus de 2,000 clés de ce type sont déjà en action de par le monde depuis juin 2007. Microsoft offre COFFEE en indiquant que la mission de l'entreprise est aussi de contrer un maximum les pirates et autres escrocs sur la toile.

Yahoo! piégé par de fausses pubs

Un pirate a affiché de fausses publicités, en avril, via le portail Internet Yahoo! Mission de ces pubs, installer des codes malicieux dans les ordinateurs des visiteurs. Les publicités, sous la forme d'une animation flash, téléchargeaient des logiciels espions.

Les internautes peu regardant sur leur sécurité informatique ont pu se faire piéger. Pour se protéger, mettre à jour ses outils de surf. Même sanction pour le site communautaire Moli.com, un portail qui offre la possibilité d'ouvrir une boutique en ligne. De fausses publicités se sont affichées.

(Protégez le cinéma, dites non aux pirates) cette campagne est diffusée en Asie. Le «master» du cinéma d'action a été demandé par la MPA locale, la MPA-i, filiale de la MPAA américaine. Une association sponsorisée par Warner, Viacom, Fox, Sony, NBC Universal et Disney. Petit problème pour Jacky. Son nouveau film, en salle en juillet, est déjà piraté sur la toile. Jacky joue au côté de Jet Li dans une comédie martiale baptisée The Forbidden Kingdom, Le Royaume interdit. Les pirates ont diffusé le DVD, début mai sur internet.

Saisie originale pour les chasseurs de pirates de film

Les policiers malaisiens ont mis la main sur une usine pirate, à quelques kilomètres de Kuala Lumpur. Jusqu'ici, rien de nouveau. Trois personnes (entre 20 et 50 ans) ont été arrêtés dans une zone industrielle. Les quinze officiers du Ministère de la consommation et du Commerce Domestiques (MDTCA), avec le soutien de la Fédération malaisienne Contre le Vol de Copyright (MFACT) et la MPAA ont saisi deux lignes de production de DVD et... 3,750 kg de polycarbonates, la matière plastique qui permet de fabriquer des DVD. Autant dire que cela risque de prendre pas mal de place dans le dossier du juge. La justice du pays indique que les lignes de production de cette usine auraient pu permettre la réalisation de sept millions de DVD contrefaits par an pour un montant de vingt-deux millions de dollars américains.



SNCF PWNED!

Un «Smiley», en tenue de Père-Noël, est apparu dans l'espace essaisasavoir.snfc.com, l'espace dédié à la coupe du monde de Rugby de la SNCF. Le pirate, qui a signé NOEL, affichait, en plus de son «personnage» un énorme «PWNED!!!». Une signature indiquant le piratage de la page. La SNCF va rapidement retirer le lien fautif qui renvoyait en fait sur le site dédié à la coupe du monde de Rugby, essaisasavoir.com. Cette page avait été piratée plusieurs fois, dont la page du fameux smiley. Si le pirate NOEL n'a pas signé son acte sur le site de la SNCF, sur le site Essai à suivre, autre méthode. La page index avait été piratée par un certain Meekaah. Il suffisait de cliquer, en même temps, sur les touches du clavier ctrl+a pour voir apparaître la signature du pirate.

LES GRANDES OREILLES DE L'ONCLE SAM ATTRAPENT UNE OTITE

Des militants pacifistes, Anzac Ploughshares, ont attaqué et dégonflé, une sphère gonflable de la base militaire de Waihopai, près de Blenheim, sur l'île sud de Nouvelle-Zélande. Les pacifistes ont percé le gros ballon de 30 mètres qui protégeait une parabole. Ils souhaitent ainsi protester contre l'activité militaire des États-Unis. Les autorités ont indiqué que cette base gère les communications par satellite et non pas un maillon du système Echelon. «Cette base est une partie importante du réseau mondial de surveillance. Nous sommes venus au nom du Prince de la Paix afin de le fermer», expliquait Anzac Ploughshares. Les grandes oreilles américaines seraient capable d'intercepter la moindre information provenant d'un téléphone portable, fax, Internet, ...



UN ESPION FILMAIT DES JEUNES FILLES SUR INTERNET

Savez-vous ce qu'est en train de faire votre petite soeur sur le web ? L'affaire qui vient de se conclure au Canada mérite de s'y attarder.

Daniel Lesiewicz, 27 ans, risque de passer les prochaines mois de sa vie derrière 4 murs. Il a été accusé d'avoir installé des logiciels espions dans les ordinateurs de jeunes filles afin de les regarder, via webcam. Parmi les victimes de ce pirate, des gamines de 14 ans qu'il menaçait des pires actions. Ces dernières étaient obligées de s'afficher nues devant leur caméra. Lesiewicz était le propriétaire d'une PME informatique et profitait de ses connaissances pour abuser des gamines. Le tribunal de Montréal lui reproche d'avoir produit des documents pédophiles. Lesiewicz trouvait ses victimes via des chats et autres forums pour adolescents. Alors, savez-vous ce qu'est en train de faire votre petite soeur ?

OMAR ET FRED S'INCLINENT FACE À DAILYMOTION

Canal+ et les deux comiques Omar & Fred n'ont pas eu gain de cause du Tribunal de Grande Instance de Paris. Comme pour le cas d'un autre humoriste, Jean-Yves Lafesse, Omar & Fred avaient attaqué le portail français Dailymotion pour la diffusion d'images tirées de leur DVD. Le journal *Écran* indique que le tribunal a rejeté les plaintes pour

contrefaçon en réaffirmant le statut d'hébergeur de Dailymotion comme il est écrit dans la L.C.E.N., la Loi pour la Confiance dans l'Économie Numérique. Omar & Fred réclamait 600.000 euros. Ils vont devoir rembourser les 5.000 euros de frais de justice de Dailymotion. Lafesse réclamait 5 millions d'euros. Il n'en touchera que 5.000 euros en dédommagement d'une vidéo retirée trop lentement.

CANAL+

DU CUL DANS LES ORDINATEURS DE LA POLICE

Conseil de discipline pour douze policiers de la ville de Québec. Nos cousins du grand nord ne rigolent plus quand cela concerne les connexions à Internet via les ordinateurs municipaux. Vingt-sept employés ont été pris la main dans le sac, en train de surfer sur des sites pour adultes. Depuis novembre dernier, quinze ont déjà reçu un sérieux



HOT NEWS

MICROSOFT VEUT INTERDIRE UN VERBE DANS LE DICO

L'utilisation du verbe «MSN-er», dans le vocabulaire des Pays-bas, pour décrire l'action d'envoyer des messages par messagerie instantanée ne sera plus permise par Microsoft Corporation. C'est du moins ce que le géant de l'informatique a imposé. Microsoft attaque en justice Carola Eppink, patronne de l'entreprise Unicaresoft. Microsoft Corporation a exigé que le dictionnaire néerlandais 'Van Dale' retire le verbe «MSN-er» de sa plus récente édition. Pourquoi ? Dans la vie courante, «MSN-er» est devenu un synonyme d'envoyer des messages par l'entremise d'un logiciel de messagerie instantanée. Microsoft exige donc maintenant le retrait de ce verbe du 'Van Dale' afin que le terme MSN ne soit plus utilisé par les autres sociétés comme marque de fabrique. Unicaresoft proposait un logiciel, MSNLock, permettant de filtrer l'utilisation de MSN.

HOUSE OF HACKERS



Une maison de hackers a été lancée, en mai. Un Myspace du hackers mis en place par le fondateur de GnuCitizen. Le but, promouvoir la collaboration entre les spécialistes de la sécurité informatique. 2.216 membres se sont inscrits en une semaine. « Ils devraient tous susciter l'admiration des citoyens pour leur travail des plus qualifié, créatif, intelligent, unique, provocateur, intense et fascinant, expliquent Petko D. Petkov (pdp), fondateur de GnuCitizen et de cette idée de Maison de Hackers, Les membres de la communauté peuvent échanger des idées, communiquer, former des groupes d'élites ou des conglomérats autour de projets. Ils peuvent également participer au marché de recrutement des hackers. Un marché conçu pour offrir des occasions d'emplois aux membres de manière juste, ouverte et libre.»

FREENET 0.7.0 DARKNET

Le projet Freenet a annoncé la sortie de Freenet0.7.0, un logiciel conçu pour garantir la libre circulation de l'information via Internet sans avoir à craindre la censure ni d'éventuelles représailles. Pour atteindre ce but, Freenet rend très difficile pour un adversaire de déterminer l'identité des personnes utilisant le réseau pour publier ou consulter des informations. Freenet est unique en son genre. C'est un réseau p2p qui dispose de son propre espace de stockage distribué accessible de manière asynchrone. Cette distribution des données sur l'ensemble du réseau le rend notamment tolérant aux pannes et aux disparitions de noeuds. <http://freenetproject.org>



coup de bâton. Cinq employés communaux ont été gratifiés d'une lettre d'avertissement, courrier inscrit dans leur dossier professionnel. Dix autres ont été suspendus, sans salaire, sur des périodes allant de cinq jours à un an. Douze policiers font parti du lot. Ils vont passer d'ici quelques semaines devant le conseil de discipline de la Police. Bilan, la ville de Québec vient de déboursé plusieurs milliers de dollars (51.000 \$ pour le système de filtrage + 11.000 \$ par an de mise à jour) pour un contrôle de ses serveurs.

6 MILLIONS DE DONNÉES CONFIDENTIELLES CHILIENNES SUR LA TOILE

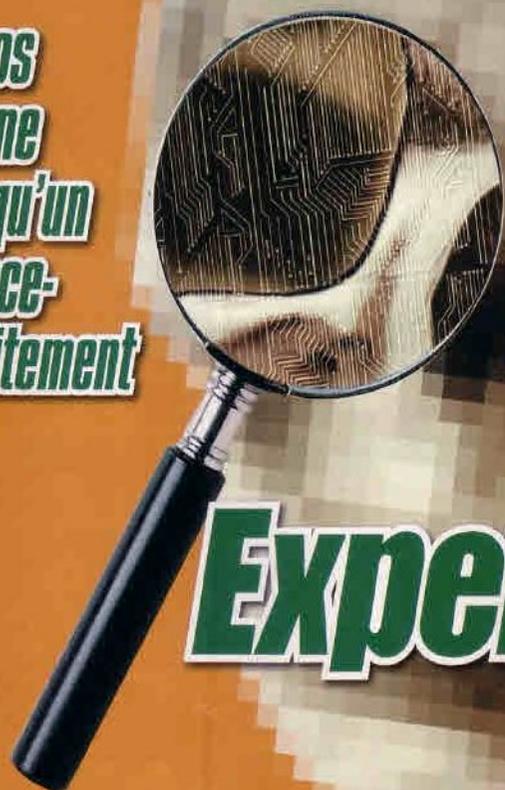
Un hacker a réussi à pirater des serveurs du gouvernement et de l'armée Chiliennes lui ouvrant les dossiers de plus de six millions de ressortissants de ce pays d'Amérique du Sud.



Numéro d'identification sociale, adresse postale, numéro de téléphone et dossier académique ont été mis en ligne par l'intrus. Sur un blog, l'informaticien a expliqué qu'il cherchait ainsi à dénoncer le laxisme des autorités chiliennes à protéger les renseignements personnels des Chiliens. Les données ont été effacées du blog. Le hacker a voulu les afficher sur d'autres blogs mais il en a été empêché. Bientôt sur le Peer-to-Peer ?

Plus fort que les

Arriver à compter vos cheveux à partir d'une photo aussi grande qu'un timbre poste... Science-fiction ??? Non, traitement de haut niveau !



Experts !

On se souvient tous, dans le film Blade Runner de Ridley Scott, d'une scène aussi célèbre que controversée : l'enquêteur Rick Deckard (Harrison Ford) remonte jusqu'à l'un des répliquants grâce à un détail crucial extrait comme par magie d'une petite photo à coups d'agrandissements et d'égalisations. Pourtant, tous ceux qui ont déjà essayé d'imprimer ou d'agrandir une photo prise sur une page web se sont heurtés à la dure réalité, bien loin des effets spéciaux d'Hollywood.

d'informations si celles-ci ne sont pas déjà présentes dans l'image... ou dans une image similaire.

:: Science-fiction ?

En l'absence de résolution adaptée, l'agrandissement d'image est une technique dont les résultats sont pour le moins frustrants. Il est certes possible de rendre certains détails plus nets, mais si l'information est absente, inutile de redimensionner, d'agrandir ou de zoomer : le résultat donnera une image floue ou dans le pire des cas de jolis pixels en gros plan. En d'autres termes, il est impossible de récupérer de grandes quantités

:: Séquences d'images

Telle est la clé de voûte d'une invention de MotionDSP (<http://www.motiondsp.com/>) qui se base non pas sur des clichés en particulier mais sur des séquences ou des vidéos dont elle parvient à récupérer des détails pour améliorer les images les plus floues. Cette technologie exploite jusqu'à 25 plans du même objet même si cinq ou six suffisent. Une vidéo ou une série de photos fera donc parfaitement l'affaire dès lors que les images ne sont



▲ La page d'accueil de MotionDSP

pas identiques et que l'angle de prise de vue varie. Résultat: il est possible de supprimer les phénomènes de distorsion et autres altérations typiques de la compression, de rendre les couleurs plus vives, mais surtout d'augmenter la résolution et les détails pour rendre lisible un texte qui auparavant était totalement flou.



:: Notre agent à Santa Cruz

MotionDSP a vu le jour en 2005, avec une technologie développée à l'Université de Californie, à Santa Cruz, même si une bonne partie des études a aussi été menée en Europe, en Serbie pour être exact. Petit détail significatif: les financements proviennent de In-Q-Tel,

un fonds d'investissement technologique de... la CIA ! Oui, vous avez bien lu, l'agence de services secrets des Etats-Unis finance publiquement des entreprises et des technologies, et MotionDSP suscite un grand intérêt auprès de ceux qui veulent faire apparaître de petits détails sur des photos floues de piètre qualité. Une vidéo avec une résolution de 320 x 240 peut ainsi donner une image avec une résolution de 1280 x 1024 pixels ou une photo panoramique.

:: Ajustez la vidéo

Heureusement, les inventions de MotionDSP ne sont pas la prérogative d'espions et autres cols blancs. FixMyMovie (<http://www.fixmymovie.com/splash/>) est ainsi disponible depuis quelques temps sous la forme d'un site web. FixMyMovie a été présenté en avant-première en automne 2007 lors de la manifestation Demo. Grâce à de nouveaux fonds, sa première version gratuite est sortie peu de temps après pour les vidéos amateur. Une fois enregistré, on peut envoyer par e-mail ou directement sur le site une vidéo dont les dimensions et la résolution maximale doivent atteindre respectivement 15 Mo et 352 x 288 (CIF): un marché qui est donc destiné aux petites vidéos réalisées avec un téléphone portable ou un appareil photo numérique bon marché.



:: Que peut-on faire ?

Parmi les améliorations numériques proposées par FixMyMovie, on retiendra la possibilité de quadrupler la résolution et d'augmenter le framerate, en passant par exemple de 7.5 à 15 images par seconde, un chiffre bien plus respectable. Parallèlement, les distorsions seront supprimées ou atténuées le plus possible, l'éclairage sera amélioré et les détails deviendront généralement plus nets. Le résultat peut ensuite être téléchargé sur votre ordinateur ou publié directement sur YouTube ou dans les espaces vidéo des bloggers ou sur MySpace.

D'INTERNET A LA TV

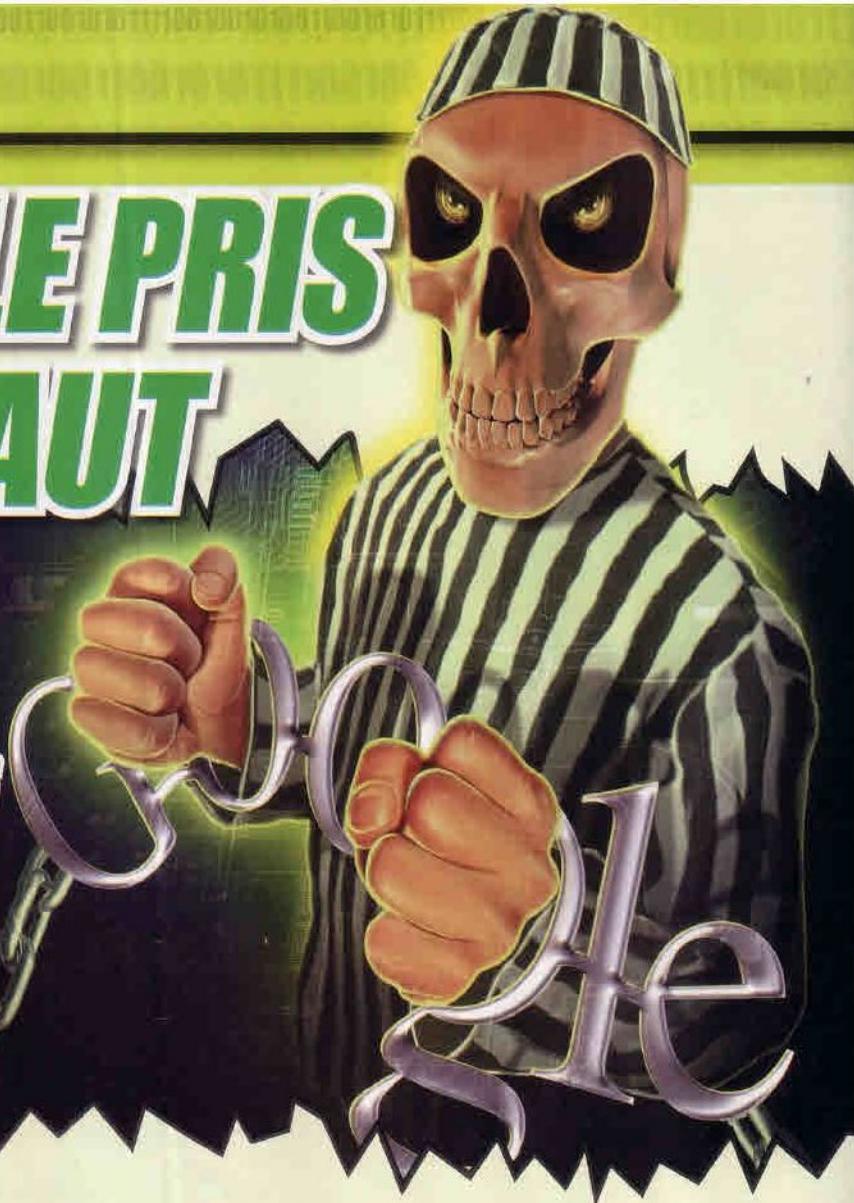
Parmi les utilisations possibles de la technologie développée par MotionDSP, la création d'un pont virtuel entre Internet et télévision. Pouvoir transférer les contenus vidéo du Net directement dans son salon numérique n'est pas dénué d'intérêt, même si l'on se heurte à certains problèmes comme une qualité insuffisante et la faible résolution des vidéos que l'on trouve sur des sites comme YouTube. Le programme d'égalisation de FixMyMovie pourrait être une solution et certaines négociations sont déjà en cours. Mais les résultats ne se verront pas immédiatement, pour une question de puissance. Actuellement, le traitement des vidéos exige beaucoup de temps, en apparaissant donc en différé. Pour obtenir des résultats en temps réel, il faudra attendre que les prochaines générations d'ordinateurs équipés de processeurs multicore deviennent plus accessibles.



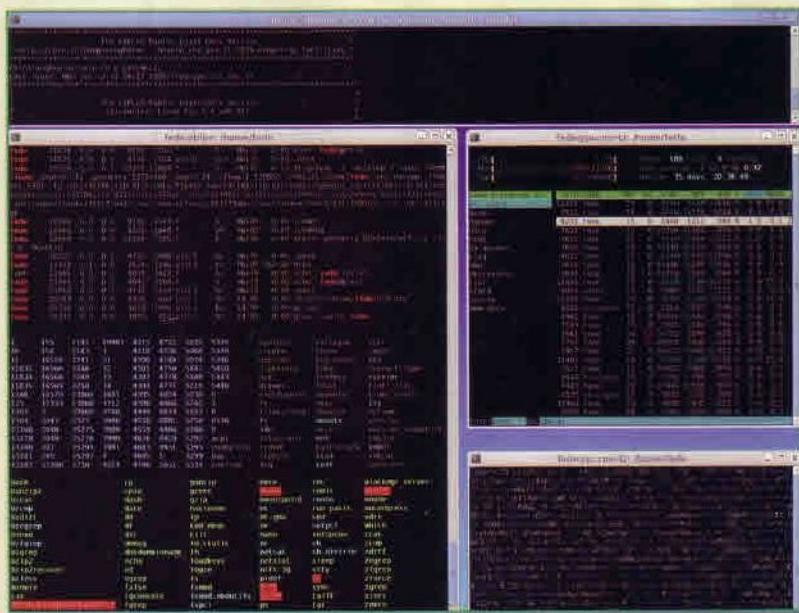
▲ Des services secrets... pour les services secrets ! Et au grand jour s'il vous plaît !

GOOGLE PRIS D'ASSAUT

Où comment rouler sans risque le plus célèbre des moteurs de recherche



Essayez d'imaginer un monde où il n'existerait qu'un seul et unique dépositaire du savoir, où quiconque aurait un seul interlocuteur, quelle que soit l'information demandée. Vous avez du mal à vous imaginer dans un tel univers ? La plupart de nos lecteurs, pour ne pas dire tous, vont spontanément chercher des informations sur Internet dès lors qu'une question leur turlupine l'esprit. Normal, me direz-vous, dans la mesure où on trouve désormais quasiment tout sur n'importe quoi, et en moins de temps qu'il ne faut pour l'écrire. Bien. À présent, concentrez-vous sur la personne que vous allez interroger et demandez-vous ce qui se passerait si quelqu'un de malintentionné décidait de ce que vous pouvez lire et, vice-versa, de ce qu'il vous est interdit de consulter, ou si cette même personne faisait en sorte de vous orienter vers des



contenus détournés, pour une raison x ou y... Combien d'entre vous arrivent jusqu'à la page cinquante des résultats de recherches ? Cacher quelque chose est encore plus facile, nul besoin de supprimer une information pour la faire disparaître : il suffit tout simplement de la reléguer en dernière position des résultats de recherche, et personne ne pourra jamais vous taxer de censure !

À présent, allons encore un peu plus loin. De nombreuses personnes estiment que le moteur de recherche de Google couvre à lui seul près de la moitié des recherches effectuées sur Internet.

Un chiffre qui, s'il est difficile à vérifier, s'avère toutefois fort plausible, compte tenu de sa forte croissance.

Que Google soit devenu la principale référence pour dénicher des informations en ligne, personne n'en doute, en devenant à ce titre l'une des plus grandes marques au monde. Google est donc synonyme d'Internet dans l'imaginaire collectif. Le réseau, la plate-forme qui permettrait à quiconque d'accéder à

toutes les connaissances que renferme ce monde, mais aussi, par certains côtés, le risque représenté par un manque évident de pluralité. Si les choses continuent ainsi, d'ici quelques années, contrôler Google pourrait devenir une véritable

manne pour certains régimes.

Et même sans aller jusque là, parions que de nombreux chefs d'entreprise caressent ce rêve inavoué pour rendre leurs concurrents quasi invisibles : tout le monde balayé en quelques clics ! Vous êtes maintenant à mi-chemin de votre parcours initiatique... maintenant, imaginez que des gens comme vous et moi puissent disposer d'un certain pouvoir sur Google.

Parfois, pour que Google apporte de l'eau à notre moulin, nul besoin de faire partie des grands noms de ce monde. Il "suffit" d'être un petit génie de l'informatique pour que Google et ses failles constituent un risque potentiel pour des millions d'internautes. Un physicien italien a récemment fait parler de lui en parvenant à pénétrer certains secrets de Google et à les retourner contre le moteur de recherche. Heureusement, il n'était animé d'aucune intention



◀ Une des ordinateurs utilisés

L'HISTOIRE VRAIE DE L'EXPLOIT SUR GOOGLE

Il y a quelques années, un peu par jeu, un peu par intérêt, j'ai commencé à étudier le fonctionnement de Google, la façon dont était indexées les pages, comment il attribuait ses notes, le critère utilisé pour juger une page plus "conforme" qu'une autre, etc... Il y a deux ans, en été, pendant mes vacances sur le Monte Rosa avec trois amis, un pari a ensuite fait le reste : réussir à placer en première page sur Google Images la photo d'un ami pendant un match de tennis. J'ai créé une page conforme aux prescriptions de Google, avec quelques trucs sur le titre, les liens et les compteurs construits spécifiquement, et j'y



ai placé une cinquantaine de photos. Le titre "Tennis de qualité" m'a bien aidé dans mon entreprise, dans la mesure où les photos dans le monde qui portent un nom pareil sont plutôt rares. Le pari était gagné. Mais le plus beau restait encore à venir. Un ami s'est aperçu que toutes les photos de la page avaient été prises par Google

en moins d'un mois et placées en toute première page des recherches, indépendamment du nom. S'il était facile pour des photos portant des noms bizarres d'être proposées en première position, il était en revanche plutôt insolite qu'une photo intitulée Ramona apparaisse en seconde position, et y reste pendant plus d'un an. Ramona était le nom de ma copine, avec qui je suis resté sept ans, et même si je trouve que c'est l'une des plus belles filles au monde (ok, je ne suis pas forcément objectif), sur cette photo elle n'avait que 16 ans (en 1988, à Brighton, UK) et elle était relativement habillée, contrairement à ses concurrentes plus pulpeuses et déshabillées ! Tel fut pour moi le véritable succès remporté sur le moteur de recherche de Google...



malveillante ou criminelle, mais uniquement poussé par le goût de la recherche, de la "découverte" des secrets de Google. Tout comme lui, nombreux sont ceux qui investissent du temps et de l'énergie pour briser les secrets du géant de Mountain View. Federico Calzolari, lui, y est parvenu. Nous l'avons rencontré pour qu'il nous raconte son exploit.



1) Décrivez-nous votre parcours personnel, ce qui vous a poussé à vous occuper de "grid computing". Parlez-nous aussi de vos centres d'intérêts.



Après avoir obtenu mon diplôme de physique et passé une année à servir la patrie en tant qu'officier de l'armée, j'ai travaillé pendant 4 ans dans le monde de l'industrie : développeur de programmes à Varèse, technicien dans un centre de calcul bancaire, puis dans une société de télécommunications. Puis je suis passé à la recherche : CNR d'abord, puis École Normale, et enfin INFN et CERN. Depuis 4 ans, je m'occupe d'architectures distribuées GRID computing, qui représentent, selon moi, l'avenir du calcul. Mes centres d'intérêt ? De la photo au sport (course à pieds et vélo), en passant par un brevet de secourisme en mer qui me sert de temps à autres, sans oublier le volontariat en

tant qu'enseignant à l'Université du troisième âge d'hiver et animateur d'activités pour enfants.



2) Pouvez-vous expliquer à nos lecteurs, sans trop entrer dans les détails, en quoi consiste une grille d'ordinateur ?



Une GRID informatisée est un ensemble hétérogène d'ordinateurs, de disques et de bandes, installés ici et là dans le monde entier, et sur lequel répartir une masse gigantesque de travail et de stockage, sans pour autant disposer localement de tout le matériel hardware nécessaire. L'idée est née du fait qu'à chaque européen qui travaille, correspond un chinois qui dort (voire 100), et dont on peut utiliser les ressources, dès lors que l'inverse est accepté et que la terre a accompli un demi-tour (ndrl : quand il fait nuit en Europe).



3) Comment décririez-vous la situation ici pour tous ceux qui sont appelés à travailler dans un milieu technique et scientifiques de haut niveau ?



Assez dramatique, pour utiliser un euphémisme. Un défi dans le défi. Une situation où, au moins une fois par an, vous devez soit remporter un concours, soit trouver des fonds pour continuer à travailler l'année suivante. En Italie, plus personne n'investit dans la recherche, qu'il s'agisse du gouvernement ou de l'industrie. Une situation peu banale !



4) Parlez-nous à présent de ce avec quoi vous avez attiré l'attention des médias. En novembre, dans le Zeitgeist de Google Italie, vous êtes apparu comme la personne la plus "recherchée", en devançant même le Père Noël. Que pouvez-vous nous dévoiler sur ce phénomène ?



C'était avant tout un jeu, qui consistait à

essayer de comprendre comment fonctionnaient les algorithmes de ranking de Google. Un problème qui n'a toujours pas été solutionné, compte tenu du blindage à toute épreuve desdits algorithmes et de la confidentialité dont ils font l'objet. Mais je m'en suis peut-être rapproché... vu le résultat. Vittorio Zambardino a bien défini cet événement : un tir dans le noir. Bien centré, serais-je tenter d'ajouter.



5) Vous avez prouvé que les craintes des gens étaient totalement fondées, et qu'il était possible de manipuler les informations sur Internet, quel que soit l'objectif à atteindre.



C'est tout à fait vrai. Raison pour laquelle j'ai utilisé mon nom et prénom, seule chose sur laquelle, en Italie, il n'existe pas de droits de copyright. Tout autre mot que j'aurais utilisé aurait été assimilé à de la publicité pour quelqu'un ou quelque chose... et aujourd'hui, j'aurais sans doute un million d'euros de plus sur mon compte ;)



6) Les responsables de Google ont semblé plutôt "amusés" de cette affaire, mais comment ont-ils pris la chose, au-delà des communiqués officiels ?



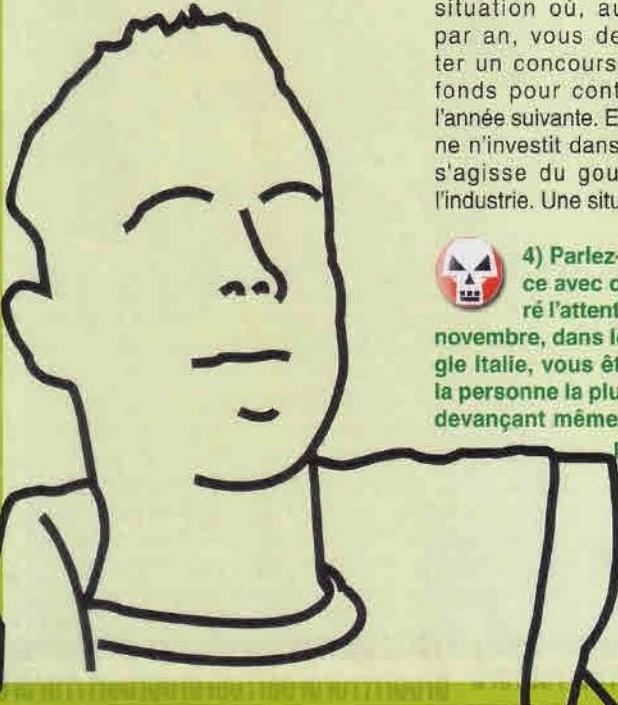
Avec beaucoup de fair-play. Après tout, reconnaître l'existence d'une petite brèche n'entache en rien la crédibilité de ce que tout le monde considère comme le meilleur moteur de recherche dans l'absolu. Je continue moi-même à l'utiliser pour mes recherches !



7) Pensez-vous qu'Internet soit destiné à devenir le principal véhicule d'information ?



Une question à un million de dollars ! Il y a quelques années, on prédisait la mort des livres et journaux. Or, les chiffres semblent démentir ces informations. Certes, Internet facilite la diffusion de la culture et de l'information, mais je ne pense pas qu'il remplacera un jour le papier imprimé. La méthode Gutenberg a encore de beaux jours devant elle.



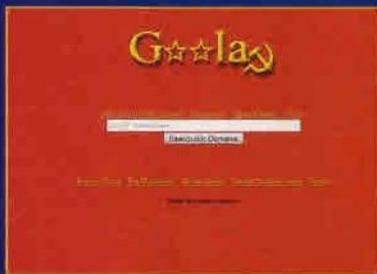
Goolag

le nouveau scanner à la sauce vache morte

Le cDc, le Cult of the dead Cow, un groupe mythique de hackers, vient de lâcher sur la toile une nouvelle petite bombe numérique qui n'a pas fini de faire causer. Baptisé Google Scanner, l'outil permet de faire remonter des vulnérabilités en exploitant le moteur de recherche américain

Les hackers du cDc ont mis en ligne GoolagScan, un scanner de site Internet à la sauce Google. Le groupe mythique de hackers, cDc (CULT OF THE DEAD COW - Le culte de la vache morte), groupe qui a édité voilà bien longtemps le premier cheval de Troie baptisé Back Orifice, vient de mettre en ligne un site Internet baptisé Goolag (GoolagScan). Mission, scanner la sécurité de votre propre site Internet en exploitant le moteur de recherche Google. «Un logiciel de vérification, explique le cDc, Le scanner Goolag permet à chacun d'auditer son propre Site Internet via Google». Goolag exploite les codes connus sous le nom de «Google Hacking», des commandes (dorks) à partir d'un formulaire mis en place par Johnny I Hack Stuff. Le scanner est encore en version bêta. Son code source est ouvert sous la licence GNU Affero. Le logiciel est à la mémoire du fondateur du Chaos Compu-

ter Club (CCC), Holland Wau, un autre grand de la communauté hacker. Goolag Scanner permet, via 1500 dorks, de retrouver des données sensibles et cachées sur des serveurs web (Cartes de crédit, mp3, mots de passe, données de configuration d'IP, ...)

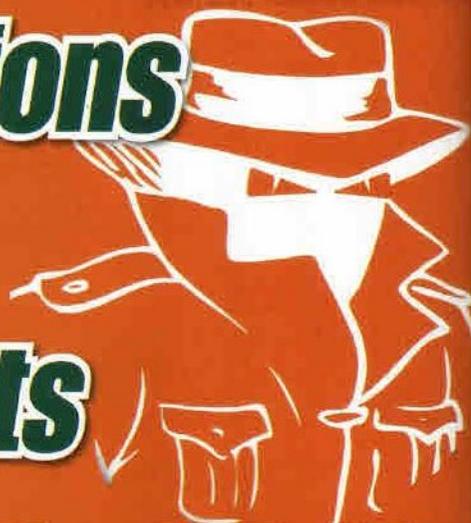


Quelques jours après sa mise en ligne, le cDc prouvait l'efficacité de sa création en annonçant avoir découvert des téra-octets de contenus pornographiques sur les serveurs Web du gouvernement Chinois. L'outil a permis de se

rendre compte que les serveurs Chinois sont mieux sécurisés que les serveurs occidentaux. «Cela suggère deux choses, explique Oxblood Ruffin, porte-parole du cDc, Un, le contenu adulte est hors de contrôle pour le Parti communiste Chinois; Deux, la sécurité des sites Internet sur les Serveurs Web gouvernementaux et militaires Chinois sont plus forts qu'à l'Ouest. A part les preuves de fichiers douteux, nous n'avons pas trouvé les mêmes vulnérabilités que nous avons pu mettre à jour aux USA, Italie ou encore en France». ■



Les jouets espions inquiètent les services secrets



Vous pensez que les jouets de votre petit frère sont inoffensifs ? Comme le grand patron de la marque automobile Porsche, vous allez très vite changer d'avis. Aujourd'hui, les jouets peuvent devenir les auxiliaires de 007. Et ce n'est plus du cinéma

Pas de doute, James Bond a du soucis à ce faire. Les gadgets permettant de mettre en place un espionnage efficace sont de plus en plus nombreux. Les matériels pour écouter, voir, bref, surveiller peuvent se cacher dans des objets étonnants. Après la crainte d'écoute via les nounours Furby. Après les espionnages via des webcams, voici venir l'écoute pirate à partir d'un babyphone. Les parents connaissent ce petit matériel qui permet d'écouter, à distance, le bébé endormi dans sa chambre.

Le grand patron de la marque automobile Porsche ne pensait pas qu'il finirait, lui aussi, sur écoute via un babyphone. L'hebdomadaire allemand Der Spiegel indiquait en avril dernier que le boss de Porsche, Wendelin Wiedeking, avait été espionné dans un hôtel de luxe, le Ritz-Carlton de Wolfsburg. L'appareil était tout simplement branché sous le fauteuil du patron. Un espionnage qui a aussi touché d'autres employés de la firme. Le responsable du comité d'entreprise a eu son portable sous écoute. Un ancien membre du directoire de Volkswagen s'est vu gratifié d'un gadget d'écoute installé dans son appartement. Bref, l'achat de Volkswagen par le constructeur automobile de luxe Porsche semble intéresser du monde.

auxiliaire d'espionnage. Pas du matos qui coutent des centaines d'euros. Encore moins des gadgets militaires. Non, nous avons fait plus simple. Nous sommes aller dans des boutiques de jouets et testé des objets qui pourraient permettre de de déjouer la moindre sécurité.

Le Détecteur Spy Micro Tracker System permet aux enfants de surveiller tous les mouvements dans une habitation. Un jouet d'enfant d'une portée de 25 mètres, qui ne coute que

:: Testé pour vous

A la rédaction de Hackers News Magazine nous avons recensé quelques matériels pouvant se transformer en



29 euros et qui reste redoutable pour celui qui souhaite surveiller un espace précis. Parfait pour s'assurer que l'espace à espionner est libre de toute personne. Un jouet qui capte même à travers les murs.

Surveiller la présence d'une personne dans une pièce, c'est bien, mais l'écouter reste votre but. Nous avons trouvé une paire de Talkie Walkie longue portée capable de renvoyer le son sur une distance de 5 kilomètres. Coût, 59 euros. Vous avez le son, vous avez le contrôle de la pièce, il vous faut quelques images. Ok, voir sans être vu ? Simple, ou presque. Les japonais de chez RF Systems viennent de sortir la caméra miniature de 2,7 Megapixels. L'œil électronique mesure seulement 3,5 cm. Les images sont envoyées en sans fil vers un boîtier disposant d'une sortie RCA. Un matos qui peut s'utiliser à distance, sans problème. Nous avons trouvé une petite TV, avec antenne intégrée, pour 50 euros, qui nous permettait de recevoir les images de cette mini caméra. Et des mini caméras, Internet en propose des centaines, plus ou moins petites. Nous avons reçu, par exemple, une «Wireless Camera». Pas plus grand qu'une balle de golf. Capable de filmer en pleine nuit et intercepter le moindre son. Coût, 80 euros.

Chez Amazon, nous avons trouvé une parabole d'écoute. Un jouet à 69 euros qui a pour mission de permettre aux enfants d'écouter la nature, les petits oiseaux. Côté test, ce matos permet d'écouter de manière correcte à une portée de 100 mètres. Intéressant, en couplant l'écoute avec le détecteur de mensonge de la société Smarthome. Voice Stress Analyzer, le nom de ce jouet, permet de savoir si la personne mise sur écoute est en train de mentir. Ce détecteur miniature analyse le niveau de stress dans la voix. Coût de la chose, 35 euros.

Dans la série surveillance sauvage, voici l'Horloge Camera Espion (Hidden Camera Spy Clock) de chez chinvasion.com. Une caméra couleur est planquée dans ce poste radio. Le récepteur reçoit

les images et permet de les enregistrer en temps réels. Un matériel passe partout qui est commercialisé 50 euros. Autre genre, pas discret avec sa grosse antenne, le Robot Espion



Snooper. Pour 40 euros, il écoute tout ce qui lui passe sous la coupole, et sur une distance de 50 mètres. D'un autre côté, qui trait s'inquiéter de ce jouer trouvé chez irobotics.com.

Du côté des lunettes, voici les «Sunglasses Camera with Personal Digital Video Recorder». Elles sont proposées par spycatcheronline.co.uk. Elles intègrent une caméra embarquée, un moniteur couleur intégré, un haut-parleur, 32Mo de mémoire interne, un port de sauvegarde pour carte mémoire SD/MMC afin de stocker plus d'images. On finira par le Détecteur d'empreintes digitales. Mieux que dans la série télévisée Les experts, le Clue Spray de la société Brevis permet de tracer les gros doigts d'un intrus sur vos documents, valises. Cet aérosol va permettre de démasquer l'espion. Ce gadget détecte les empreintes digitales. «Appliquez le spray sur un objet, celui qui sera manipulé en secret par la personne soupçonnée. Vous croyez que l'objet a été touché ? Utilisez une lampe ultra-violette pour voir les empreintes digitales» explique

l'inventeur. Un spray commercialisé moins de 20 euros. Bref, quelques matériels tout à fait capable d'être exploités par des personnes mal intentionnées. Les Mac Gyver de l'espionnage n'ont plus qu'à détourner ces jouets et gadget pour en tirer profit. Alors la prochaine fois que vous regardez votre petit frère, assurez-vous qu'il n'a pas planqué une de ses voitures ou nounours dans votre bureau. ■



LA GUERRE DES CB: l'attaque des clones

En France, 6.000 porteurs de cartes bancaires se font pirater, chaque jour.

Comment est-ce possible ?

Comment agissent les fraudeurs ?

Hacker News Magazine a mené

l'enquête dans un monde où

le cash coule à flot. Exclusif!



Benjamin (un pseudo) à 23 ans. Ce jeune étudiant Suisse ne se doutait pas qu'en ce beau lundi de décembre il finirait entre 4 policiers, menottes aux poignets, direction les bureaux gris d'un commissariat. Tout a débuté pour lui en 2006, sur

le web. « Je surfais, explique-t-il, et j'ai rencontré des gens. Nous causions de tout et de rien quand l'un d'eux a proposé du matériel électronique un peu spécial ». Un matériel d'autant plus spécial. Benjamin s'en rendra compte au commissariat, que ce dernier coûtait pas moins de 3,000 euros. « Je n'avais pas les moyens de l'acheter, ni vraiment l'envie de jouer avec le feu. Mais le fait d'avoir été en contact avec ce vendeur. La police a voulu m'entendre ». Mais que vendait donc cet étrange interlocuteur pour que les forces de l'ordre sortent la grosse artillerie ? De la drogue ? Des armes ? Non, Benjamin venait de croiser la route d'un commerçant particulier, revendeur de matériel skimmer.

Les skimmers ? De petits boîtiers en plastique bourrés d'électroniques. Comme l'expliquait déjà la revue interne Mission de la Police Nationale (N°82 –

2004) Les pirates « utilisaient d'authentiques distributeurs automatiques de billets (DAB) pour contrefaire les cartes bancaires des clients effectuant des retraits d'espèces. (...) Des dispositifs difficilement repérables pour un œil non averti, (...) recueillaient les informations confidentielles des cartes : un appareil (...) placé devant la fente du distributeur, lisait la piste magnétique de la carte, tandis qu'une caméra dissimulée dans le plafond (...)



Des skimmers pour recopier la bande magnétique de la CB.





Les pirates font dans l'international avec des claviers par pays.

enregistrait le code secret composé par la victime. » Une méthode qui n'a pas changé. 4 ans plus tard, elle s'est modernisée et professionnalisée. Nous avons pu rentrer en contact avec l'un de ces revendeurs. Les skimmers sont revendus entre 3000 et 3500 dollars. Les faux claviers, les Pinpads, 1.500 dollars. Pour ce prix, l'acquéreur a en sa possession le lecteur/enregistreur de carte, un faux clavier d'interception des mots de passe et un logiciel qui permet de cloner, parfaitement, la carte interceptée. Du matériel de pro qui permet de fabriquer de parfaits clones des cartes, baptisés White plastic, White card. A la différence des Yes card, qui n'existent plus aujourd'hui, les White card demandent toujours un mot de passe valide. Les revendeurs proposent donc clavier et/ou mini caméra. En France, 6.000 fraudes ont lieu par jour. Il faut dire aussi que les français utilisent 2 fois plus leur carte bancaire que le reste

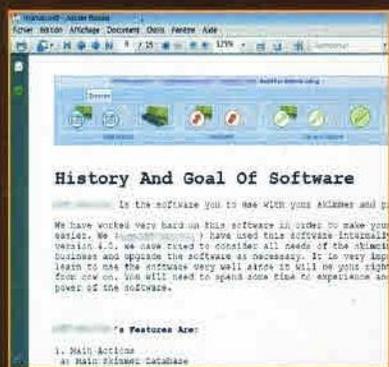
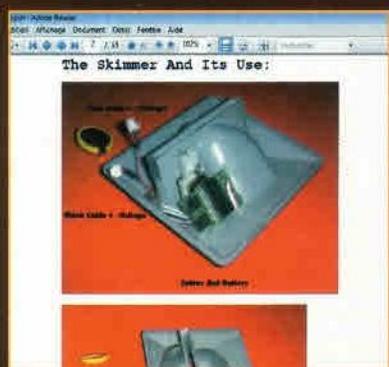
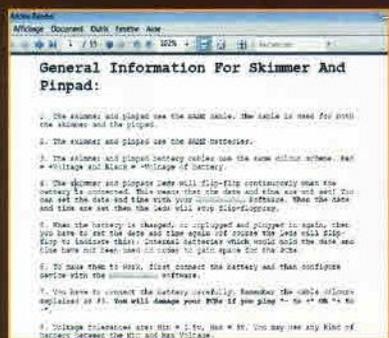
des européens. Une fois sur deux, les victimes ont toujours leur carte bancaire, donc sans destitution, au moment où les pirates ponctionnent le compte en banque. En une heure, les données bancaires piratées seront acheminées par Internet (IRC, MSN, ...) vers d'autres pirates qui voleront l'argent, effectueront des achats frauduleux.

Pour se protéger, rien de plus simple. Vérifier toujours qu'aucun dispositif mouvant ne se trouve sur les lecteurs de carte bancaire que l'on peut rencontrer sur les distributeurs de billets, pompe à essence ou autres machines urbaines. Cachez toujours vos doigts quand vous tapez votre mot de passe (Inutile si un faux clavier remplace la mini caméra pirate). Dans tous les cas, déposer plainte et prévenez rapidement votre banque.

Damien Bancal



▲ Un faux clavier pour intercepter le mot de passe.



▲ Mode d'emploi fourni avec le matériel

Prochainement sur vos écrans :

FIRMWARE 2.0

Nos fins limiers sont partis à la recherche du nouveau firmware (sortie prévue en juin), destiné au petit bijou téléphonique de chez Apple. Et il l'ont trouvé !!!



C'est à San Francisco que se déroulera du 9 au 13 juin prochain le World-wide Developers Conference (WWDC). Un rendez-vous annuel à ne pas manquer, fixé par Apple pour présenter les toutes dernières nouveautés de ses produits, avec une session spécifique consacrée à l'iPhone et à la nouvelle version de son système d'exploitation.

Mais pour les développeurs et quelques chanceux, la version bêta (early beta) du nouveau firmware est déjà disponible ! Une mise à jour qui sera sans nul doute délivrée sous le nom de firmware 2.0. Mais rien n'est moins sûr ! Car il n'est pas dit qu'Apple change ensuite d'avis et introduise des versions intermédiaires, du style 1.1.5 ou 1.2. Pour ceux qui ont pu les étudier de plus

près, les fonctionnalités du firmware 2.0 sont très intéressantes : les caractéristiques multimédia de l'iPhone se sont améliorées et s'adressent désormais aux entreprises, un milieu où semble régner en maître le Blackberry de la Research In Motion (RIM).



Apple vient en effet d'acheter et d'intégrer dans son prochain firmware la licence d'ActiveSync de Microsoft, qui permettra à l'iPhone de se synchroniser avec Microsoft Exchange Server 2003 et 2007 (standard pour de nombreuses entreprises). Cette nouvelle fonctionnalité permettra ainsi à l'utilisateur de lire son courrier électronique professionnel, de gérer ses rendez-vous, échéances et planifications, comme s'il était physiquement à son bureau.

Pour protéger les connexions entre l'iPhone et le serveur de l'entreprise, ces dernières doivent obligatoirement passer par un canal crypté, et le Virtual Private Network (VPN) est la technologie adaptée à ce genre de service. Dans les images présentes sur le réseau, parmi les options proposées dans la configuration des VPN à bord de l'iPhone, apparaît également le logo du VPN IPsec de Cisco, premier fournisseur mondial de solutions réseaux pour Internet. Un partenariat qui garantit ainsi le professionnalisme requis dans une connexion protégée.

Et il semblerait même que Microsoft ne soit pas du tout indifférent au succès rencontré par le petit bijou d'Apple. D'ailleurs, ces jours-ci, Tom Gibbons, vice-président de la division de Microsoft consacrée aux périphériques et applications, laisse justement entendre dans une interview accordée à Fortune, qu'ils étudient de près le marché qui gravite autour de l'iPhone. But de cette étude ? Proposer dès que possible un portage de leurs produits (et le bruit court qu'une version de Microsoft Office pour iPhone

serait déjà en chantier). Il y a donc fort à parier que certaines applications pour iPhone dites Office-ready seront déjà délivrées dès juin, en permettant donc de lire les formats Word et Excel sans toutefois pouvoir les éditer. Bien sûr, l'iPhone a apporté de grandes nouveautés sur un marché jusqu'à présent dominé par des périphériques tournant sous WindowsCE, Symbian et BlackBerry. Microsoft souhaite donc sans doute devancer d'éventuels concurrents en essayant d'imposer ses produits soft-

(la nouvelle interface du nouveau firmware présente une touche consacrée à App Store).

L'idée d'Apple est simple : délivrer un Software Developer Kit (SDK) totalement gratuit pour permettre aux utilisateurs de développer un software tant pour l'iPhone que pour l'iPod, moyennant la somme de 99 dollars. Les développeurs tiers pourront revendre leur propre software par le biais du magasin officiel d'Apple. Les frais d'inscription comprennent le support technique et toute la documentation fournie par Apple.

Apple retiendra 30 % des ventes sur toute application basée sur son App Store, tandis que le développeur tiers encaissera les 70 % restants. Pour les applications freeware, un espace totalement gratuit sera en revanche proposé. La production de software s'en trouve ainsi stimulée, qu'elle provienne de professionnels ou d'amateurs, en leur donnant la possibilité d'être sponsorisés par une multinationale de premier ordre, à un coût franchement abordable (surtout pour nous européens, avec le change qui est en notre faveur). Le magasin online d'Apple sera donc sans doute présenté officiellement lors du WWDC, et il y a de fortes chances pour que les développeurs et experts IT découvrent lors de cet événement toutes les possibilités qui leur seront proposées.

Mais voyons maintenant quelles devraient être les autres fonctionnalités



ware sur une plate-forme prometteuse, où elle n'a pas (encore) le monopole. Autre nouveauté intéressante (toujours attendue dès juin) : la possibilité d'installer d'autres softwares, en les achetant directement à partir de son iPhone par le biais d'iTunes App Store, le magasin online d'Apple



CRACK 1.0

Certains se souviendront sans doute du tollé suscité par le crack de la protection des DVD (appelé DeCSS), peu de temps après l'accord passé entre les différents producteurs mondiaux quant au standard définitif à adopter pour distribuer et vendre les films. L'auteur du crack, Jon Lech Johansen, a été surnommé depuis DVD Jon et c'est également lui qui a contourné (ou comme on dit sur le réseau, débloqué) la protection de l'iPhone. Grâce au talent de ce jeune norvégien, l'iPhone qui serait normalement contraint de fonctionner avec les seules cartes sim du gestionnaire de téléphone américain AT&T, peut en revanche fonctionner avec n'importe quelle carte sim, y compris celles françaises. Il existe différents tutoriels sur le réseau qui vont jusqu'à la version 1.1.4 et qui expliquent pas à pas la façon de débloquent son iPhone.

introduites, déjà dévoilées ou découvertes en lisant les chaînes présentes dans le firmware :

- la recherche parmi les contacts ne s'active pas immédiatement, mais uniquement lorsque le nombre de contacts enregistrés devient élevé (la loupe Spotlight apparaît) ;
- l'application Calendrier présente un nouveau bouton qui n'est pas encore actif. De même pour le bouton qui permettra de se connecter à l'App Store ;
- le Contrôle parental, qui permet de limiter les contenus exploitables par les mineurs, fonctionne quant à lui à la perfection ;
- l'utilisateur pourra réorganiser les réseaux Wi-Fi selon ses préférences ; l'application Bonjour (déjà connue des utilisateurs Mac), a ensuite été insérée pour permettre de connecter en toute simplicité plusieurs périphériques entre eux sur le même réseau Wi-Fi (et au dire de nombreuses personnes qui l'utilisent déjà, il semblerait qu'elle soit irremplaçable) ;
- la Calculatrice est beaucoup plus évoluée : si vous lancez l'application lorsque l'iPhone est en position verticale, la calculatrice standard vous sera alors

proposée, mais si l'application est déjà lancée et que vous tournez l'iPhone en position horizontale, vous passerez alors en mode scientifique. En outre, les touches ont été redessinées puisqu'elles sont désormais carrées ;

- l'utilisateur pourra enfin sélectionner plusieurs messages à la fois dans l'application Mail pour les supprimer, les copier ou encore les déplacer ;
- le mode plein écran sera désormais disponible tant pour le navigateur Safari que pour chaque application, et Safari supportera enfin les vidéos de YouTube (on ne sait pas encore si cela s'effectuera avec un plugin créé spécifiquement ou directement par le biais du navigateur) ;
- les technologies de graphiques vectoriels adaptables (SVG) ont été intégrées : l'utilisateur pourra ainsi bénéficier d'images de grande qualité encore plus légères. De nouveaux effets CSS ont également été introduits ;
- intégration du support pour les présentations PowerPoint (au format pps) ;

La version 2.0 proposerait enfin le support du service fort coûteux .Mac d'Apple qui permet d'intégrer une messagerie électronique, de sauvegarder des documents Mac, de créer des galeries photos online, des disques durs virtuels et bien d'autres choses encore... En effet, en analysant les chaînes présentes dans le firmware, on peut lire "Syncing with this Dot Mac account will turn off syncing for other Dot Mac accounts and delete any existing synced data".

Outre ces nouveautés plutôt géniales (pour lesquelles il faudra toutefois attendre le lancement officiel du nouveau firmware, puisqu'elles n'apparaissent que dans les captures d'écran présentes dans le SDK et dans les présentations d'Apple), certaines rumeurs plutôt sérieuses affirment que le nouvel iPhone d'Apple deviendrait compatible avec les réseaux haut débit mobile 3G (UMTS).

Une nouvelle version de l'iPhone qui serait présentée lors du lancement du nouveau firmware. A dire vrai, cette rumeur circule depuis pas mal de temps sur le réseau, mais Ken Dulaney, un analyste de chez Gartner, a déclaré ces derniers jours qu'Apple avait commandé 10 millions de terminaux 3G. On parlerait même de la présence de la technologie OLED (celle-là même qui a été inaugurée dans certains des tout derniers téléphones portables SonyEricsson et Motorola) pour réaliser sans doute un iPhone

beaucoup plus fin. Si ces infos étaient confirmées, l'engouement battrait alors son plein, non seulement outre-atlantique où les iPhone sont vendus depuis longtemps (même s'ils sont officiellement bloqués sur le réseau d'AT&T, voir encart), mais aussi sur le marché européen où la version actuelle de l'iPhone n'a pas rencontré le succès escompté (hors USA, on ne le trouverait presque exclusivement que sur ebay). L'Europe s'est en effet lancée depuis longtemps dans les connexions haut débit par le biais de réseaux mobiles (chez nous, on parle désormais de 3,5G et 4G) et de nombreuses personnes ont considéré l'absence de cette connectivité sur l'iPhone comme un grave handicap. D'après certaines indiscretions, trois variantes d'iPhone 3G seraient proposées : une de 8 Go (à 399 dollars), une de 16 Go (à 499 dollars) et une de 32 Go (à 599 dollars). Concrètement, un smartphone et un disque dur portables à utiliser également pour télécharger des contenus multimédia à bande large, le tout signé Apple. On parle d'indiscretions car Apple n'a délivré aucun communiqué à cet égard. Attention donc au prochain rendez-vous du WWDC et comme on dit dans ce cas, stay tuned !

CRACK 2.0 - BETA -

Le firmware 2.0 n'est pas encore sorti que le DevTeam a déjà montré comment contourner les protections d'Apple pour faire tourner sur l'iPhone d'autres applications non certifiées par la multinationale. Concrètement, l'équipe a réalisé une version modifiée du boot code du téléphone qui permet d'intercepter le contrôle de l'iPhone avant que le système d'exploitation ne le fasse. Cette possibilité ouvre ainsi de nombreuses perspectives, parmi lesquelles la libre expérimentation. Leur projet s'appelle Pwnage et sa version 1.1 vient juste de sortir : elle supporte la dernière build du firmware pour iPhone (5A240d). En outre, leur site propose les codes modifiés en accès libre et leur outil corrige également un bug du firmware d'Apple relatif à la gestion WiFi.

Attaque graphique

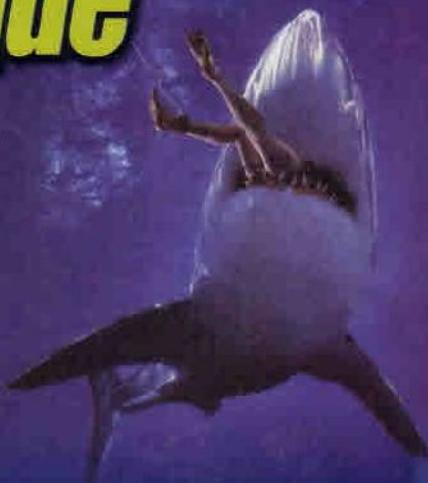
Un informaticien français propose sur Internet une étude passionnante sur le crackage d'un mot de passe au format MD5 en couplant CPU et GPU

Il existe pléthore de systèmes sur la toile permettant de « casser » un mot de passe chiffré en MD5. L'idée de Benjamin Vernoux, alias Titan, n'est pas d'être The Master of the World, mais plutôt de travailler et étudier une possibilité exploitant les ressources de nos ordinateurs. Il vient de réaliser un petit outil permettant de « cracker » un mot de passe au format MD5. « J'ai mis trois jours pour le réaliser, confie Benjamin, Environ une journée pour créer une maquette sans interface graphique, puis portage sous MFC et l'optimisation ma prise environ 2 jours. » Pourquoi un tel projet ? « Je dirais tout simplement pour le challenge et la recherche de l'optimisation ultime du couple CPU/GPU, explique-t-il, Ça me rappelle la bonne vieille époque de la programmation sur Amiga avec le Copper/Blitter... la programmation était optimisée et les programmes/jeux étaient rapides

et très réactif. A l'image de l'AmigaOS qui est pour moi toujours un référence au niveau réactivité pour un OS.»

La première bêta du logiciel tiré de l'étude de Titan tournait à environ 20 Millions de hash MD5/sec, sans aucune optimisation particulière, seul l'algorithme MD5 a été porté sur CUDA 1.1 (GPU) pour tourner de manière parallèle. Le fonctionnement est assez novateur. Côté CPU, l'outil calcul un brute force (36 possibilités a-z et 0-9) et prépare le MD5 avec un résultat de 64 octets par mot de passe « Ce calcul est fait par block de 2 millions de mot de passe (soit 128MB) » explique Benjamin. L'outil copie des mots de passe type MD5 vers la mémoire GPU (Graphics Processing Unit), la carte graphique. Le GPU calcul le MD5 de chaque mot de passe et vérifie si le HASH correspond au hash à trouver « Si le hash est trouvé, on met un flag à 1 et le hash trouvé en mémoire GPU que le CPU vérifiera ».

Les diverses optimisations du générateur de brute force côté CPU avec une réécriture complète de l'algorithme de brute force en fonction des tailles de mot de passe, côté GPU l'auteur de cet outil est passé à 30 Millions de hash MD5/sec. La version proposée sur le site Internet de Benjamin Vernoux, la Version 0.1, a eu une optimisation de la bande passante. « Les mots de



passes calculés côté CPU sont stockés sur 16 octets à la place de 64 octets plus utilisation de la mémoire CPU CUDA en mode - pinned - 20% plus rapide, mode normal environ 2.1GB/sec, mode pinned 2.5GB/s ». La v1.0 a eu aussi une optimisation de l'algorithme MD5 côté GPU « utilisation des vecteurs pour charger les mots de passe par block de 128bits avec suppression des conflits ». La prochaine étape du travail de cet informaticien va consister à déplacer une grande partie du brute force dans le GPU qui au passage à une bande passante de plus de 47GBytes/sec sur une GeForce 8800GT « Alors que la bande passante mémoire CPU n'est que d'environ 2.5GBytes/sec ». Voilà une belle étude informatique qui devrait intéresser les passionnés de codage et de chiffrement. La version actuelle fait un brute force sur 36 caractères (les lettres a à z avec les chiffres de 0 à 9).

Le logiciel et l'étude sont accessibles sur <http://bvernoux.free.fr/md5/index.php> ■



L'ELDORADO des pirates

Les programmes antivirus vivent des "heures sombres", du moins c'est ce que confirme une enquête de Panda Security. Voilà pourquoi, vous n'êtes plus en sécurité...

Un ordinateur sur quatre est infecté et ce, même s'il est protégé par un antivirus. Dans les réseaux d'entreprises, en revanche, la proportion atteint même des chiffres records : trois LAN infectées sur quatre. Ces données proviennent d'une enquête réalisée par Panda Security et met en exergue un phénomène que de nombreux spécialistes de sécurité avaient déjà dénoncé depuis fort longtemps : face aux perpétuels assauts des virus informatiques, les softwares de sécurité perdent du terrain !

:: Une nouvelle ère

Les temps ont changé et, avec eux,

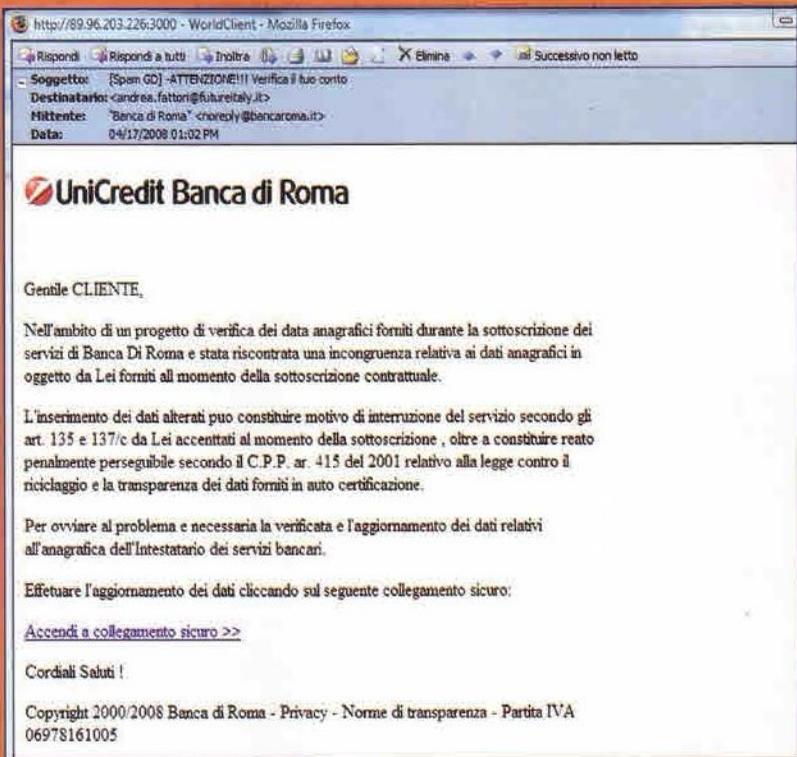
le type de menaces tapi dans le Web. S'il y a encore quelques années, le pirate informatique dégagait une image romantique, celle du "génie incompris" cherchant à se venger de l'entreprise qui l'avait maltraité ou qui agissait dans le simple but de devenir célèbre, aujourd'hui ceux qui écrivent des virus informatiques n'ont plus qu'une seule idée en tête : gagner de l'argent. Une évolution que l'on doit surtout au développement d'Internet et à l'utilisation massive de cartes de crédit sur le Web. Ces dernières représentent en effet une part extrêmement appétissante pour ceux qui possèdent les connaissances nécessaires pour créer et diffuser des virus. D'après les données diffusées par Panda Security, 20 %

des virus identifiés en 2007 étaient des chevaux de troie, à savoir des virus destinés à permettre le contrôle à distance de l'ordinateur infecté. Une fonction souvent utilisée pour dérober des informations confidentielles.

:: Gangs criminelles

Mais dans ce genre d'affaire, rares sont les pirates qui agissent seuls. Le marché des virus implique en effet de véritables "gangs" criminels qui opèrent dans les bas-fonds d'Internet pour réaliser leurs gains. Aujourd'hui, ceux qui souhaitent gagner de l'argent avec le crime informatique, n'ont même plus besoin de connaissances informatiques

particulièrement approfondies : il suffit juste d'avoir les bons contacts. Sur le Web, en effet, vous pouvez acheter un virus flambant neuf pour ensuite le diffuser. But du jeu : infecter le plus grand nombre de PC pour obtenir un botnet, à savoir un réseau d'ordinateurs contrôlables à distance, prêts à exécuter toute opération à l'insu du propriétaire légitime. Même le fonctionnement des virus s'est "affiné". Après avoir pris le contrôle du PC infecté, le criminel de service dispose d'une interface graphique qui lui permet de contrôler des centaines d'ordinateurs simultanément. Il utilise également des filtres qui sélectionnent les machines à utiliser en fonction des critères les plus disparates, tels que le pays où elles se trouvent. Il peut donc décider d'activer tous les ordinateurs



PROTÉGÉS MAIS PAS INFECTÉS

La campagne de Panda Security s'appelle Infected or not et a été lancée suite à une étude qui a analysé un million et demi d'ordinateurs déjà protégés par un antivirus. L'analyse a été menée en utilisant une base de données comprenant 11 millions de virus. Les résultats sont désarmants : en effet, 22,97 % des PC analysés, étaient infectés. Un chiffre qui grimpe à 35 % lorsqu'il s'agit d'ordinateurs dont le système de protection n'a pas été mis à jour. L'analyse sur les réseaux d'entreprises, révèle ensuite des données encore plus alarmantes : 72 % des réseaux sont infectés. Le système de scan online est ouvert à tous à l'adresse suivante : www.infectedornot.com et n'exige qu'une rapide procédure d'enregistrement.



▲ Si votre PC est infecté, il peut alors être utilisé pour envoyer des spams ou, pire encore, des messages qui tentent d'attirer de nouvelles victimes sur des sites de phishing. Ici soit disant pour une banque italienne

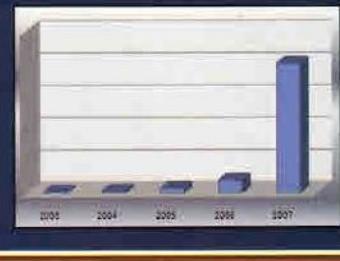
contrôlés en Espagne pour lancer une campagne de spams, ou utiliser tous les PC infectés situés en Australie pour lancer une attaque contre un site Web spécifique.

:: Au plus offrant

Mais la chaîne du crime informatique ne s'arrête pas là. Il y a en effet peu de chances pour que ceux qui gèrent un botnet prennent des risques à titre personnel. Les pirates informatiques de "seconde génération" préfèrent en effet travailler pour d'autres personnes, en vendant leurs services sur des sites spécialisés. Des sites qui vous permettent de commander l'envoi de spams ou même une attaque contre le site Internet d'une entreprise concurrente. Même les informations sur les cartes de crédit que les pirates parviennent à dérober, ne sont pas utilisées

CROISSANCE EXPONENTIELLE

Ces dernières années, les fabricants d'antivirus ont enregistré des millions de nouveaux virus. L'aspect le plus inquiétant reste toutefois le taux de croissance de nouvelles versions : en 2007, on a en effet relevé 10 fois plus de nouveaux virus qu'en 2006. Mais le type de virus change également. En effet, les trojan se multiplient, utilisés pour contrôler à distance les PC et voler des informations. En 2005, ils ne représentaient que 49 % du total des nouveaux virus détectés, 63 % en 2006 et jusqu'à 75 % en 2007.



► En naviguant sur Internet, vous pouvez trouver des dizaines de sites qui proposent des services liés à l'utilisation de spyware et adware.

sur-le-champ. Elles sont en effet revendues à d'autres organisations qui se chargent de faire fructifier l'investissement à travers certains stratagèmes qui leur garantissent l'immunité. Il s'agit de véritables "sociétés" spécialisées, qui recrutent via Internet des gens naïfs disposés à effectuer des "transactions financières". Concrètement, les personnes piégées doivent ouvrir un compte courant dans une banque, recevoir des sommes d'argent, retenir un tout petit pourcentage de ces sommes et envoyer le reste à l'étranger. Les pays de destination, souvent situés en Europe de l'Est, sont choisis selon des critères très précis : ce sont tous

des pays où les enquêtes ont de fortes chances de ne jamais aboutir.

L'opération permet de "blanchir" l'argent, en faisant en sorte que les intermédiaires recrutés (nos fameux pigeons !) pour recevoir et envoyer l'argent soient les seuls que les forces de l'ordre puissent retrouver.



:: Sournois

Mais comment tout cela influe-t-il sur le fonctionnement des antivirus ? Ce type d'organisation a également bouleversé les objectifs des auteurs de malwares. Les virus d'ancienne génération étaient programmés pour être le plus visible possible : ils bloquaient l'ordinateur, affichaient des messages menaçants ou spirituels, provoquaient des dysfonctionnements qui révélaient immédiatement leur présence. Aujourd'hui, en revanche, un "bon" virus doit passer inaperçu, s'installer sans endommager l'ordinateur et agir dans l'ombre pour faire gagner de l'argent à son créateur. Ce n'est pas un hasard si 75 % des virus apparus en 2007 sont des chevaux de troie, une famille de virus qui ne peut pas se diffuser de façon autonome mais qui permet à son auteur de contrôler la machine à distance. Mais les pirates informatiques ont également adopté d'autres stratégies qui ont semé la panique auprès des fabricants d'antivirus, en rendant leur travail extrêmement difficile.

DANS LA LIGNE DE MIRE DES CRIMINELS

Une fois le virus diffusé, les pirates informatiques peuvent contrôler tous les ordinateurs infectés d'un seul endroit. Leur système de contrôle est tout sauf spartiate : il

permet de répartir les ordinateurs par nationalité, d'envoyer des commandes spécifiques et d'afficher des statistiques détaillées concernant l'activité de chaque groupe de PC.

MPack v0.90 stats

Attacked hosts (total - uniq)		Traffic (total - uniq)	
IE XP ALL	114721 - 96104	Total traff	159073 - 129089
QuickTime	2179 - 2048	Exploited	44804 - 35574
Win2000	7033 - 6260	Loads count	17408 - 15968
Firefox	12885 - 12514	Loader's response	38.85% - 44.89%
Opera7	1271 - 1264	Efficiency	10.94% - 12.37%

Browser stats (total)		Modules state	
MSIE	4 (0%)	Statistic type	MySQL-based
Opera	1 (0%)	User blocking	ON
		Country blocking	

Country	Traffic	Loads	Efficiency
RU - Russian federation	112793 (70.9%)	12653 (72.7%)	11.22%
UA - Ukraine	16666 (10.5%)	1670 (9.6%)	10.02%
IT - Italy	7045 (4.4%)	593 (3.4%)	8.42%
GE - Georgia	5775 (3.6%)	673 (3.9%)	11.65%
BY - Belarus	5419 (3.4%)	657 (3.8%)	12.12%
KZ - Kazakhstan	3098 (1.9%)	376 (2.2%)	12.14%
US - United states	1117 (0.7%)	50 (0.3%)	4.48%
AZ - Azerbaijan	1060 (0.7%)	128 (0.7%)	12.08%
MD - Moldova republic of	683 (0.4%)	101 (0.6%)	14.70%

:: Points faibles

Les programmes antivirus utilisent différentes techniques pour détecter les programmes dangereux. Les plus évolués se basent sur l'analyse des opérations accomplies par les programmes, mais exigent l'utilisation de nombreuses ressources et ralentissent énormément l'ordinateur. La technique la plus utilisée reste donc celle des définitions : le programme antivirus analyse

LIKES SOFTWARE
интерактивный программ**ЛИСИЯ**
ЛУЧШАЯ БОЛЬШЕ!

пакетный коп-ва продаж

андартных 15\$ до 20\$

le code des fichiers et le comparé avec une base de données renfermant les virus connus.

Premier point faible de ce système : la création de la base de données. En effet, pour qu'un virus soit reconnu, il faut absolument que le fabricant d'antivirus en

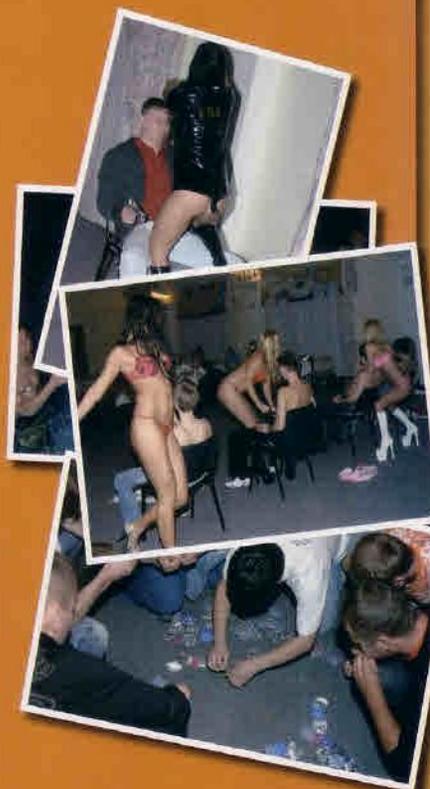
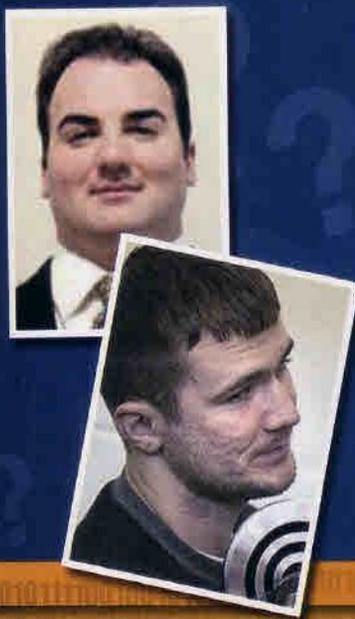
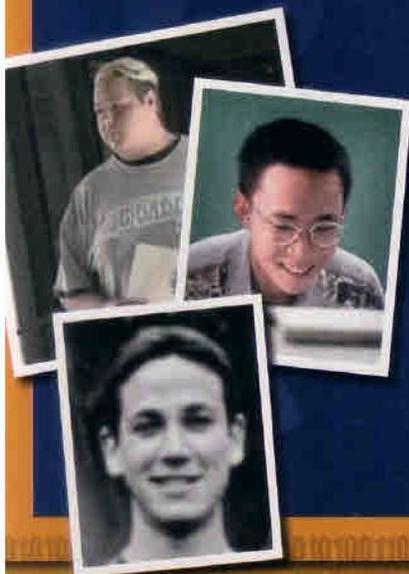
reçoive un "exemplaire", appelé dans le jargon sample. Les samples proviennent des sources les plus diverses : des signalements des utilisateurs qui ont installé l'antivirus, d'autres sociétés spécialisées dans la sécurité informatique et des honeypot, des ordinateurs connectés au Web et destinés à "attirer"

▲ Le site www.infectedornot.com permet d'analyser le PC pour vérifier l'éventuelle présence de virus "cachés"

PORTRAITROBOT

Souvent, il suffit de regarder une personne en face pour savoir à qui l'on a affaire. Dans le cas des pirates informatiques, il suffit de jeter un œil à ces photos d'archives pour comprendre à quel point les choses ont changé. A gauche, les auteurs de virus com-

me Blaster, Sasser et NetSky. Il s'agit de jeunes programmeurs qui ont agi pour accéder à la notoriété ou, dans certains cas, par pure inconscience. A droite, en revanche, les portraits de deux pirates arrêtés pour phishing et spams au cours de ces derniers mois.



▲ Quelques images capturées lors de la "convention des pirates russes". Dans la vie, il n'y a pas que les virus ;)

INFECTED



[Main](#) | [PeaDuCT](#) | [SOCKS v.4/5](#) | [D.D.o.S SERVICES](#) | [SpAM SERVICES](#) | [Arpma SpAM BoT](#) | [ABOUT](#) | [FoRUM](#)

[WEB-Tools](#) | [English Version](#) | [Google Search](#)

MaIN MENU

- [Main](#)
- [PeaDuCT](#)
- [SOCKS v.4/5](#)
- [D.D.o.S SERVICE](#)
- [SpAM SERVICE](#)
- [Arpma SpAM BoT](#)
- [ABOUT](#)
- [FoRUM](#)



INFECTED

FreND'S-SITE

- [Socks 5 Service](#)
- [OpenTeam.Info](#)
- [MHackers.RU](#)
- [MINI-RINGE.RU](#)
- [Anonymous.RU](#)
- [\[:::FL0DD3R.RU:::\]](#)
- [\[:::bviok.net:::\]](#)
- [black code's page](#)
- [WWW.AXXY.RU](#)
- [CesLab Team](#)
- [Samouchka.Net](#)
- [PrivateNATtack.ru](#)
- [White-hacker.org](#)
- [COMP-INFO.RU](#)
- [Cyber Crime](#)
- [HackInfo.org](#)
- [Root-Access.RU](#)
- [BugFinder.INFO](#)
- [\[:::KZ Team:::\]](#)

NEWS

»»» [Завершена разработка Автооплаты на сайте WWW.SOCKS.RU](#)

Теперь вам нет необходимости оплачивать тарифный план или стучать в аську если Вам

► Pour vendre leurs "services", les pirates informatiques utilisent des sites Web normaux. A partir de là, vous pouvez commander l'envoi de spams dans un pays spécifique ou demander une attaque Denial of Services contre un site

les virus et à se laisser infecter pour permettre aux experts de les analyser. Si le labo du fabricant ne reçoit pas de sample, l'antivirus sera incapable de reconnaître le malware. Second point faible : la taille de la base de données. D'après une récente étude, environ 11 millions de virus, trojan et spyware circulerait sur le web. Des archives qui les renfermeraient tous seraient extrêmement "encombrantes" et la comparaison engendrerait une masse de travail trop importante pour le processeur.

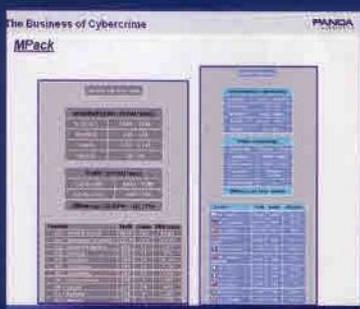
C'est pourquoi, les bases de données des antivirus vendus dans le commerce n'intègrent que les virus les plus dangereux et répandus, mais ne vous protègent pas contre les moins connus. Enfin, la plupart des fabricants d'antivirus s'appuient encore sur une analyse "manuelle" des samples, qui sont étudiés par des experts pour évaluer leur éventuelle dangerosité. Une sorte de procédé "artisanal" caractérisé par une sempiternelle lutte contre le temps.

:: Hors contrôle

Les pirates informatiques frappent justement en exploitant ces faiblesses, en augmentant de façon exponentielle le nombre de variantes de chaque virus et en réduisant leur diffusion. Concrètement, au cours de ces 18 derniers mois, de nombreux virus différents sont apparus, dont chacun n'a frappé que quelques centaines d'ordinateurs. Parmi les techniques utilisées, on trouve également des systèmes de compression et d'encryptage qui modifient radicalement l'aspect du code sans toucher aux fonctions. Une technique qui désarme totalement les systèmes basés sur des définitions. Les cyber-criminels ont ainsi atteint un double objectif : d'un côté, ils ont "engorgé" les bases de données des fabricants d'antivirus, tandis que de l'autre, ils ont réduit les risques de voir leurs virus détectés et analysés. D'après les données de nombreux experts, plus de 15 000 nouveaux samples surgissent tous les jours sur le Web. Une masse qu'il est presque impossible de classer à temps.

SANS SE SALIR LES MAINS

De nombreux pirates ne font même pas l'effort de contrôler personnellement les informations qu'ils sont parvenus à dérober. Ils se contentent d'enregistrer les Logs générés par les trojan, à savoir l'enregistrement de toutes les opérations accomplies par le PC infecté, en les revendant ensuite à d'autres personnes. Le système de paiement s'effectue "au poids" : 30 dollars pour 50 Mo de données.



Les contre-mesures

Pour combattre cette offensive, de nombreuses sociétés antivirus se sont mises à développer des systèmes alternatifs, pour répondre plus rapidement et efficacement à la vague de virus qui traverse le Web. Les stratégies sont toutefois très différentes. De nombreux fabricants misent en effet sur des systèmes qui analysent les fonctions des programmes, en adoptant un système dit heuristique. Sophos et Panda Security se distinguent en revanche des autres, puisqu'ils ont tous deux réalisé un système pour l'analyse automatique des samples, en réduisant ainsi l'intervention humaine aux seuls cas où

le serveur qui analyse les fichiers a un "doute" sur la dangerosité du software.

Nouvelle solution

Automatiser l'analyse des fichiers permet de proposer une réponse plus rapide lorsqu'on reçoit des samples, mais ne facilite pas leur découverte. Panda Security remédie à ce problème à travers l'Intelligence collective, un principe très intéressant, du moins sur le papier. Concrètement, l'antivirus active une procédure spécifique chaque fois qu'un nouveau processus "apparaît" sur la machine. Mais l'analyse du processus au sein du PC, n'est pas particulièrement approfondie : elle est en revanche demandée via Internet à un groupe de serveurs spécialisés, qui analysent le programme pour établir s'il s'agit ou non d'un virus.

Les informations ainsi obtenues sont enregistrées et forment une sorte de "base de données à distance". Lorsqu'un autre ordinateur avec antivirus Panda signalera l'apparition de ce même processus, la réponse ne se fera pas attendre. Grâce à cette technique, l'Intelligence

COMBIEN GAGNENT-ILS ?

Les activités des pirates informatiques de nouvelle génération sont extrêmement lucratives. Dans l'un des cas récemment analysés par les experts en sécurité, l'organisation démantelée était capable de contrôler plus de 70 000 ordinateurs infectés. En calculant les gains pays par pays, on atteint un total d'environ 850 000 dollars par mois.

collective devrait être capable de détecter également les virus les moins répandus, en allant ainsi combler une "faille" qui, aujourd'hui, permet aux pirates informatiques d'agir en toute impunité.

La guerre continue

Pour vérifier l'efficacité d'un système comme l'Intelligence collective développé par Panda Security, il faudra un peu de temps et il est fort probable qu'en cas de succès, d'autres fabricants d'antivirus suivront une voie semblable. Reste à savoir quelles seront les contre-attaques des pirates informatiques, qui pourraient par exemple miser sur un renforcement des rootkits, à savoir ces programmes capables de "cacher" un processus au système d'exploitation. La partie est donc loin d'être finie !



Dans de nombreux cas, les activités des pirates sont tout sauf clandestines : cette photo montrant le fruit de l'activité des pirates a été tranquillement publiée sur le site officiel de la société

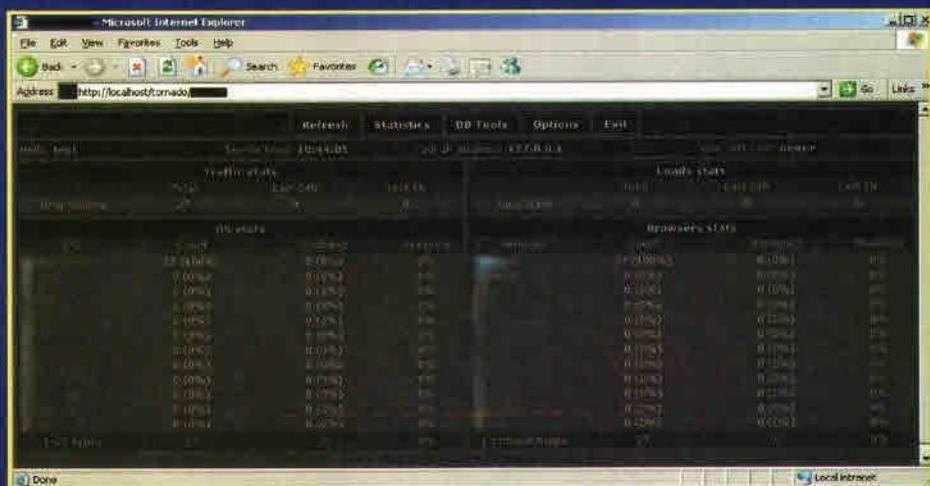
LE MARCHÉ NOIR

Voici une liste des prix moyens pratiqués pour l'achat d'informations volées par le biais de trojan. Parmi les "biens" disponibles, on trouve également les comptes de jeux vidéo populaires online tels que World of Warcraft, vendus à des prix faramineux, et même ceux du programme populaire messenger ICQ. Sur le Web, en effet, les comptes bénéficiant de chiffres "bas" d'ICQ, à savoir ceux à 6 ou 7 chiffres, s'arrachent à prix d'or !

- Compte FTP
- Compte ICQ
- Compte d'un commerce online
- Cartes de crédit VISA ou Mastercard
- Passeports en noir et blanc
- Passeports couleur

- 1 dollar
- Entre 1 et 10 dollars
- 50 dollars
- de 1,50 à 2 dollars
- 2 dollars
- 5 dollars





Symantec a du mettre la main sur cet outil normalement commercialisé dans certains forums russes.

Une fois installé, Tornado s'exploite comme IcePack. Après avoir rentré un login et un mot de passe, l'outil s'administre comme un logiciel Internet de base. Cette administration va ensuite attendre les données envoyées par d'autres pages. Car tout le piège consiste en deux temps. Le second est assez simple, le pirate doit installer un code dans des sites qu'il aura préalablement piraté. ce code aura pour mission de piéger les visiteurs des dits sites compromis. Chaque visiteur risque de se faire infecter ensuite par les codes malicieux de Tornado dans la mesure où il est faillible à l'une des 14 failles exploitée par la tornade noire.

Une redirection pirate qui fait fureur sur la toile depuis plusieurs mois.

Des sites comme Monster, Virgin, Reporter Sans Frontière, des ambassades ont été touchées par ce piège. Des cas qui prouvent que Tornado n'est pas unique et que cette famille d'outils pirates n'a pas fini de faire des petits. «C'est simple, confirme un T0fx, un expert en la matière, aujourd'hui c'est l'automatisation des logiciels pirates. L'intrus installe et laisse faire la technique. Je connais même des cas où les pirates réceptionnent les données par SMS». Des outils qui sont commercialisées, entre 100 et 1.000 dollars selon les options, les possibilités, ... Les serveurs infectés peuvent aussi se louer. Bref, la mondialisation à la sauce pirate a pris de l'avance. «Avec ce modèle, explique Liam O'Murchu

de chez Symantec, les créateurs de l'outil peuvent le vendre à quelques clients de confiance à un prix élevé, au lieu de le distribuer à de nombreux clients douteux et de risquer de voir le code publié dans l'ombre.»

www.symantec.com/enterprise/security_response/weblog/2008/04/tornado_on_the_loose.html

:: Sortez couvert face aux tornades

Attention, ce type d'outil sort de l'ombre jamais par hasard. Souvent, les anciennes versions sont lâchées dans la e-nature pour des motifs très précis. «Soit les vendeurs veulent mettre en avant leur savoir faire, confirme t0fx, soit ils piégent leur création pour ensuite mettre la main sur de pseudo pirates qui se feront eux même piégés». Bref, Tornado n'a rien d'exceptionnel mais montre que les avancés technologiques pirates sont de plus en plus efficace. L'une des options de Tornado, en plus d'infecter les visiteurs, de récupérer cookies, les ips, ... est aussi de faire croire qu'il n'existe pas. Si vous tombez sur un serveur qui cache en son sein Tornado, votre navigateur affichera une erreur de connexion. Comment se protéger de ce type d'attaque. Aussi idiot que cela puisse paraître, il est très simple de se protéger de Tornado et de sa bande. Mettez à jour vos logiciels de navigations, vos Os, un firewall et le tour est joué. Même si une page est infectée, vous ne risquez rien. ■

Les pirates Chinois médailles d'or du piratage ?

Des pirates chinois auraient attaqué l'Internet pour manifester leurs mécontentements face aux divers propos sur les droits de l'homme en Chine

在这里，我的心再也不用担惊受怕

从篱笆上眺望无限的空间，



沉落在这无穷无尽的天宇；

从篱笆上眺望无限的空间，

Les pirates Chinois sont-ils des idiots ? Les soldats numériques de la grande muraille ont-ils tapé sur la toile comme de simple script Kiddies ? Des Denis Distribués de Service (DDoS) ou autres codes viraux sans proxies ? Des «hackers» du pays du soleil du milieu se seraient attaqué aux sites et serveurs Internet appartenant aux groupes occidentaux

appartenant à des pays ayant traité des droits de l'homme en Chine. Fin avril, par exemple, un code viral avait été diffusé à partir du site de Reporters Sans Frontières. Un logiciel espion téléchargé à partir d'un site Taiwanais. « Une administration pirate avait même été installée » nous confirmera le service presse de RSF. Le distributeur Carrefour menaçait par un DDoS.

La chaîne d'information CNN attaquée; ... Des dizaines de sites infiltrés. Et tout ce petit monde, avec des ips venant de Chine. « Des attaques de grandes ampleurs venue de chine mais aussi a l'aide de Bots sont survenus sur les sites Carrefour, dans le monde » nous confiait une source de la rédaction. Pas discrète l'attaque ? Les bots exploitaient des IP contrôlés par des Fournisseur



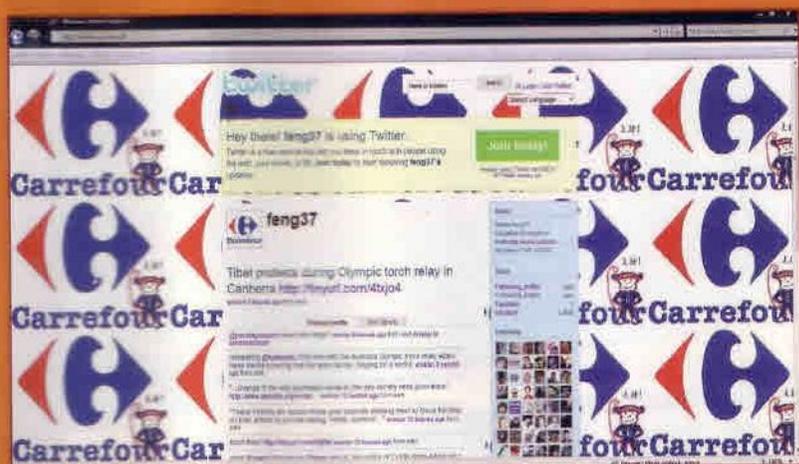
temporairement inaccessible. Nous sommes désolés des désagréments que cela occasionnent et nous espérons être de retour dès que possible ».

Les pirates, tous des chinois ?

Les services secrets de l'Oncle Sam parlent de pirates âgés entre 20 et 25 ans, des étudiants. HackCNN va diffuser plusieurs logiciels afin de perturber CNN. Des programmes diffusés par www.hackcnn.com. Le site a

été fermé. Le premier, baptisé AntiCNN, exe permettait de noyer le serveur CNN de requête de http. Le second, Sdos, exe offrait la possibilité de spécifier un serveur et un port d'attaque. Une boucle de données inondait ensuite le TGP du site attaqué. Le troisième logiciel est piégé. «Une backdoor qui pourrait permettre au pirate diffuseur de piéger les pirates utilisateurs, confirmait Jose Nazario de la société Arbor Networks. Alors, Chinoise ou pas Chinoise ses attaques ? Il est tout de même étonnant que les «pirates» et autres «hackers» chinois ne connaissent pas

d'Accès à Internet Chinois. Étrange et tellement simpliste. De son côté, la chaîne américaine CNN aura été touchée plusieurs fois par des attaques DDoS. Fin avril, trois jours d'attaques. Des tentatives de blocage de petites envergures qui n'ont pas particulièrement gêné le site américain même si ce dernier a dû fermer quelques heures son portail sport. Un groupe de «hacktivistes» est cité dans cette attaque. Baptisé HackCNN, ces derniers ont mis en ligne un site web proposant des logiciels «pirates» pour lancer des DDoS. La page «Sport Network» (sports.si.cnn.com - sport-network.com/) a été gratifiée d'un «Tibet was, is, and always will be a part of China!» (Le Tibet appartient à la Chine et ça ne changera pas) du plus bel effet. CNN a dû fermer cette espace durant 24 heures en affichant un message laconique d'excuse : «Sports Network, ainsi que d'autres grands sites d'actualités, ont été attaqués par une entité politique de Chine, et de ce fait, est



le b.a ba de l'intrusion qui est... d'utiliser des proxys. C'est un peu comme si vous aviez en main des accès à la banque de France. Que vous étiez capable d'y rentrer sans être vue, de vous servir dans les coffres. Mais pour agir, vous préféreriez sortir votre costume à paillette, sauce Disco et que vous inscririez votre identité sur une pancarte autour de votre cou. Le tout, en allant braquer la banque, en pleine journée, bien entendu. Même le plus idiot des script-kiddies n'agirait pas ainsi, alors imaginez des pirates à la solde du gouvernement de Pékin !

D. B.