Piratage - Virus - Sécurité - Hacking - Phreaking - Carding - SPAM

ZATAZ MAGAZINE

n°1 Janvier - Fevrier - Mars 2002

Microsoft vous espionne !
Comment éliminer facilement les mouchards de Windows

12F

EXCLUSIF

Matignon piraté !

Comment les communications officielles ont été interceptées
Le détail des intrusions dans l'Intranet de Matignon

Télévision : Canal Plus GRATUIT

PMU : Piratez comme vous aimez !

Fausses cartes bancaires le nouveau fléau

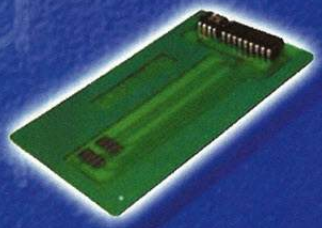
M 5129 - 1 H - 12,00 F - 1,83 € - RD

Trimestriel - 12 FF - Belgique : 85 BEF - Suisse : 4,00 CHF - http://mag.zataz.com

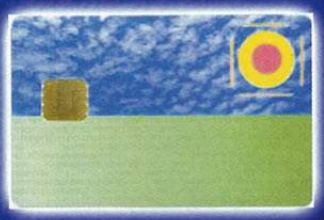
europsx.com

ARRETEZ D'ACHETER TROP CHER !!

Cartes-Programmateurs-Composants-Modchips



WaferCard
- 16F84
- 24LC16
- Supports à souder



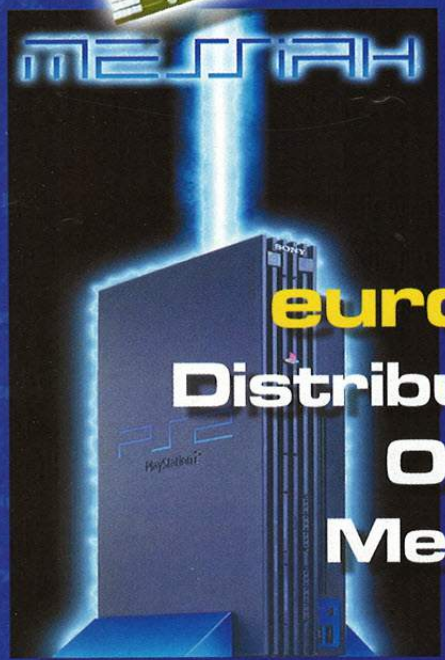
FunCard v2.0
- AT90S8515
- 24LC64

GoldCard
- 16F84
- 24LC16

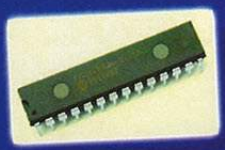
SilverCard
- 16F877
- 24LC64

"N'attendez rien du Père Noel !
Les cadeaux sont sur europsx.com"

Puces
modification
- PSX, PSOne, PS2



Pièces détachées
- PSX, PSOne, PS2
- Blocs optiques
- Alimentation



Composants
- Pic 16F84A
- 24LC16
- Pic 16F876
- Pic 12C508
- Programmateurs
- ...

Pas de frais de port - Pas de minimum de commande

Paiement sécurisé CB

Plus d'infos: info@europsx.com ou www.europsx.com

n°1

Sommaire

Bienvenue !

Il était une fois un magazine électronique qui vit le jour à la fin des années 80. D'abord appelé Croco Computer Club sur Amstrad CPC puis Cocoon sur Atari ou encore HES sur Amiga. En 1998, ce magazine se lance sur la toile, il se nomme ZATAZ.COM

Aujourd'hui, nous sommes heureux et fiers de vous présenter la version papier de ce magazine. News, reportages exclusifs, ateliers, ZATAZ Magazine est maintenant le complément indispensable de sa version électronique.

En contact régulier avec les plus grands acteurs de la scène Pirates du monde entier, nous avons la primeur des informations et sommes ainsi en mesure de vous présenter des dossiers inédits, comme dans ce numéro l'histoire ahurissante du piratage des serveurs de Matignon ou bien celle des fausses cartes banquaires que nous avons réussi à nous procurer.

Notre objectif n'est pas de publier une revue sombre où têtes de mort rivalisent avec bandes dessinées mais de vous proposer une revue colorée, agréable à lire, demystifiant et analysant chaque trimestre le monde du piratage et du Hacking.

Je vous souhaite une excellente lecture !

Damien Bancal

une publication

MEDIA Stone

http://mag.zataz.com

Zataz Magazine 61, rue Jouffroy d'Abbans, F-75017 Paris , Fax : 01.40.53.86.44 magazine@zataz.com

Directeur de la Publication : Charles Daleau
Chef de la rédaction : Damien Bancal
Ont collaboré à ce n° : Benoit Guignard, Eric Romang, Antoine Santo, LaurentZ, Replicant, Geek Girl, Jasper, Benjamin Seguillon, Willhem Canaris.
Impression Leonce Deprez, Béthune
Distribution : NMPP **N° de Commission paritaire** : 0900 K 78431 **ISSN** : 286-496X. Dépot légal à parution.

Magazine trimestriel édité par : Mediastone
Siret : 42990015200019 -
Code APE : 221 E

Toute l'actualité du hacking et du piratage !

actu!

Planète Underground

SAUVEGARDEZ VOS DVD

La cour d'appel de Californie a tranché au sujet de la copie de DVD. Dans son dernier jugement, rendu le 1er novembre, le tribunal a autorisé la publication des codes du logiciel DeCSS permettant de reproduire un DVD. Entre liberté d'expression et protection des droits d'auteurs, on ne doute pas que les majors du cinoche US ne vont pas en rester là.

OpenDVD.org

CYBER IDITOTIE

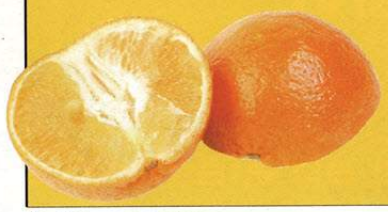
Des script-kiddies ont attaqué un groupe Usenet dédié à l'Islam via une technique de mail-bombing. L'administrateur de oc.religion.islam a ainsi du faire face à cette attaque de masse contre son serveur pendant tout un week-end. Les pirates se sont déclarés «membres d'un groupe d'autodéfense».

FAUX .BMP, VRAI VIRUS

Attention à ce ver Bitmap qui arrive par e-mail sous le nom de ***me.bmp***, un soit disant dessin au format BMP. Le message vous demande de modifier son préfixe en .com (ben voyons!), puis de l'exécuter. Il infectera alors votre logiciel IRC, pour peu que vous en ayez un. Il s'agit bien là d'une des virus les plus pitoyables que nous ayons pu voir !

LES SPAMMES VOIENT ORANGE

L'opérateur de réseau mobile, ORANGE accusé de SPAM ? Il a été constaté que des revendeurs affiliés à Orange envoyaient des messages SMS non-sollicités aux téléphones des clients appartenant à d'autres réseaux concurrents. "Ces appels n'ont pas été effectués par les services marketing d'Orange" a expliqué un porte-parole Orange. Pendant ce temps, certains consommateurs voient rouge !



Sony lève la papatte

Photo : Sony

Selon un article dans « The New Scientist», des programmeurs ont donné une nouvelle fonctionnalité au chien électronique de Sony, **Aibo**. Ces bidouilleurs ont appelé cette fonction «Disco Aibo» et permet de faire danser le chien robotisé au son de n'importe quelle musique. Cela n'a pas fait rire du tout Sony qui a demandé que soit enlever le programme *illico presto* des robots appartenant pourtant à des particuliers. Motif ? Le code du clébard est chiffré et surtout il est sous copyright. Rappelons qu'en 1999, le Furby, animal électronique de chez Hasbro, avait été interdit par le FBI dans les lieux administratifs sensibles. L'animal poilu pouvait en effet être modifié par des pirates en micro-espion !

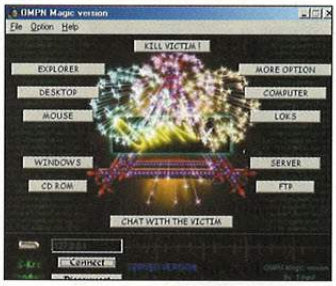
FBI vs Terroristes

Le FBI qui souhaitait placer son outil espion Carnivore chez plusieurs fournisseurs US pour «traquer» les terroristes s'est fait gentillement reconduire par la plupart des FAI. Earthlink par exemple, qui est l'un des plus importants fournisseurs d'accès a expliqué qu'il avait son propre outil, sans apporter plus de précisions. Nous comprenons toutefois l'intérêt du FBI : les terroristes avaient en effet utilisé des comptes Internet un peu partout qu'ils utilisaient via des bibliothèques municipales, notamment dans des bibliothèques publiques du Comté de Broward, en Floride. Des centaines de messages électroniques en anglais et en arabe entre les pirates de l'air présumés et leurs complices ont déjà été découverts. Rappelons enfin qu'après le premier attentat du World Trade Center en 1993, le FBI a trouvé des fichiers chiffrés dans l'ordinateur portable de Ramzi Yousef, le leader reconnu coupable de cet attentat. Ces fichiers décrivaient précisément l'attaque de 11 avions de ligne commerciaux américains. La grande majorité de ces fichiers étaient cryptées avec P.G.P.

Nation Unis qui mal y pense

L'équipe de ZATAZ Magazine a mis la main sur un serveur des Nations Unis faillible. Et pas à n'importe quelle faille puisqu'elle concerne Unicode, ce problème *made by Windows* qui a fait les beaux jours des script-kiddies cet été 2001, sans parler de l'utilisation de la même faille par les virii Code red et Nimda. On a cru rêver quand l'accès au disque dur de ce serveur nous a été possible. Nous les avons contacté la délégation Indienne a qui appartient ce serveur. Ils ont rapidement corrigé la faille mais semble être trop timides pour nous remercier !

Un nouveau trojan français nommé OMPN



Ce cheval de Troie, réalisé par *Titant*, tire son nom de l'Orphelinat Mutualiste de la Police Nationale, l'auteur ne manque pas d'humour. Ce trojan tourne via le port 452 car d'après son géniteur «Mon numéro de lingerie là-bas». Après quelques tests, il s'avère qu'aucun de nos antivirus ne l'ont détecté. Ce programme existe en plusieurs versions avec un client variant, en taille, de 200 kilos à plus d'un méga. L'outil, simple d'utilisation, permet de forcer un chat avec la victime, changer de résolution de l'écran, faire du bruit, bloquer son navigateur, son PC. Bref, une arme à ne pas mettre en toutes les mains.

12

C'est en milliards de dollars ce que les virii auraient causé de dégâts cette année. Une baisse de 5 milliards par rapport à l'an 2000. L'étude en question provient du "Computer Economics Inc.

Pas cher mon frère !

Après les sites pornos qui se battent pour avoir comme nom de domaine Ben Ladden, voici le tour du site Al Qaida de se voir récupérer... pour être revendu. L'internaute qui a mis la main sur ce domaine en demande plus de 100.000 dollars. Il nous a affirmé que l'argent serait reversé aux associations d'aides aux victimes. C'est cela même...!

Ali baba ouvre-toi

Deux étudiants en informatique de l'Université de Cambridge, Michel Bond et Richard Clayton, ont constaté que le logiciel qui protège les distributeurs de billets de banque contient un défaut qui pourrait être utilisé par un employé malhonnête. Le bug permettrait de forcer les codes secrets et de lire les informations lors de la transaction bancaire avec le GAB, le guichet automatique de billets. IBM, dont le système a été mis en cause, affirme qu'il n'y a aucun problème en raison de la multitude de sécurités mise en place. Les deux étudiants ont quand même réussi à forcer les codes de chiffrage stockés sur un IBM 4758, machine certifiée par le gouvernement américain en 1998.

COCA-COLA FORMULAS

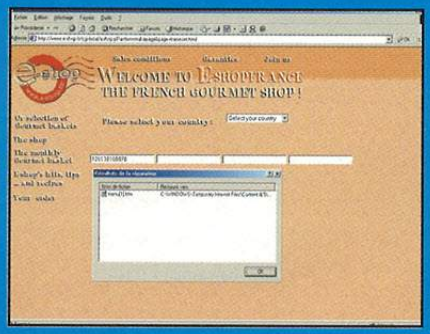
Voici peut être la prochaine révolution qui protégera les écrits papier. Une société israélienne basée à Tel-Aviv vient de développer une batterie qui peut être imprimée directement sur du papier. Cette pile minuscule pourra servir à une multitude de produits allant du livre à la carte bancaire en passant par des patches médicaux intelligents ou des cartes d'embarquements d'avions sécurisés. Le projet est tellement secret, que la formule a été nommée «Coca Formulas» en raison du secret qu'entretient, elle aussi, la marque de boisson gazeuse autours de son breuvage.

SACRE JOE !

Un nouveau logiciel découvert par des internautes, nommé "Voyage Alpha Force" serait prêt à frapper le web. Le programme permet de préparer une attaque de type DoS. Cette alerte fait suite aux autres alertes d'une future attaque de masse. Pour Noël ? Ce «logiciel» se propage comme un ver et joue, comme Nimda ou Code Red, avec les «mauvaises» configurations de Microsoft SQL Server. VAF se propage via un programme nommé JOE.EXE qui appelle par la suite un chat irc penr0x.

DANGER VIRUS

Le site de E-commerce e-shop.fr tente d'installer sur votre machine le virus Nimda lors de votre connexion. Un conseil, évitez donc de vous rendre sur cette page. Nous avons contacté le webmaster qui semble, lui aussi, trop timide pour répondre. En espérant qu'au moment où vous lirez ces lignes le site aura été soigné.



Toute l'actualité du hacking et du piratage !

actu!

Planète Underground

PLAYBOY A POIL

Le site Playboy vient d'avouer que son serveur avait été visité et qu'un pirate, nommé "Martin Luther Ping" avait mis la main sur des numéros de cartes bancaire de clients du journal. Le groupe «ingreslock 1524», dont fait parti M. Ping, a expliqué qu'il avait accès au site depuis 1998 !

BOULETTE AU FIGARO

Suite à une boulette les abonnés de la newsletter du FIGARO ont reçu jeudi 1er novembre un e-mail leur demandant d'effacer un logiciel de leur PC. Le courrier provenait d'un internaute qui était destiné aux administrateurs de la lettre d'information du site. Ce message reprenait mot pour mot le hoax sulfnbk. La direction du Figaro nous a fait savoir que « toutes les mesures ont été prises afin qu'un tel incident ne se reproduise pas ».

L'EUROPE ET LES PIRATES

29 Etats, membres du Conseil de l'Europe ainsi que le Japon, Les Etats-Unis et le Canada, ont signé la Convention internationale de lutte contre la cyber criminalité. L'objectif de cette convention est de limiter l'activité criminelle sur Internet. Dans les grandes lignes : la contrefaçon de logiciels, escroqueries à la carte bancaire, virus informatique, la pédophilie en ligne...

WAREZ ET JUSTICE

Un étudiant de 20 ans qui vendait des copies de logiciels pour Playstation vient d'être attrapé. Le tribunal a décidé de le condamner à 10.000 FF d'amende. Amende jugée insuffisante par Le Syndicat des Editeurs qui s'était constitué partie civile et avait demandé 3 fois plus. Le juge a, heureusement pour l'étudiant, ramené l'amende à 10. 000 F avec sursis et à 4 700 F de dommages et intérêts.

Rendez-vous sur le site de Zataz Magazine !

http://mag.zataz.com

Joyeux noel ...

Comme chaque année, à quelques jours de noel, les éditeurs de jeux vidéo trouvent un moyen de faire parler d'eux sans débourser un rond dans la publicité ! Comment ? En communiquant sur des arrestations de pirates de logiciels. Le dernier exemple en date, la descente du FBI et des douanes US dans les universités le 11 décembre dernier. Une opération appelée «Boucanier» qui a permis à la police de perquisitionner et saisir des disques durs sur les campus de 21 Etats américains. Le réseau de pirates nommés «DrinkOrDie» (boire ou mourir, ndlr), était composé d'étudiants chevronnés, de spécialistes de la programmation mais aussi d'employés de sociétés qui recellaient certains programmes sous licence pour les diffuser, à leur manière, dans le domaine public. Ce groupe existait depuis 1993.

Wanadoo piraté ?

Pendant quelques heures la page Bourse de Wanadoo a affiché un texte pas comme les autres. Dans un dossier intitulé: «Placements : Comment réagir face à la crise ?», un message, qui n'avait pas grand chose à voir avec les placements boursiers, demandait de l'aide pour les plus démunis. Les propos étaient en faveur plus précisement des familles Tsiganes qui tentent de vivre en France.

règle n°1 : Ne jamais défier des hackers !

Unbreakable, incassable. C'est sous cet adjectif qu'ont été présentés les logiciels d'Oracle dans la dernière publicité en date. il n'en fallait pas plus pour pousser des milliers de hackers à prouver le contraire ! De 3.000 attaques hebdomadaire, le site d'Oracle en accuse maintenant plus de 30.000...et pas une seule de réussie...Ben alors les gars, on fatigue ? Qui de vous fera cet exploit ? :-)

Ne touchez pas 20 000 francs

Il était beau, grand, fort, mais il est surtout très con. Un ingénieur en informatique âgé de 26 ans n'avait pas prévu que les sociétés qu'il volait avec des fausses cartes bancaires allaient lui tendre un piège. Patrick Azzouzi, patron toulousain d'une boutique de vidéo en a eu marre qu'un voleur vienne lui barboter sous le nez des cassettes et des DVD via ses distributeurs automatiques. Après plus d'une dizaine de plaintes sans résultats, il a décidé de regarder lui même sa série de cassettes vidéos personnelles, celles qui surveillaient ses distributeurs de films. Et, dimanche soir, après trois jours d'attentes, la police a enfin pu mettre la main sur le voleur et l'une des cartes de crédit falsifiée. Le malfaiteur a été placé en garde à vue à la gendarmerie de Tournefeuille.

Traceur de GSM

Belles migraines pour les 70 % d'Irlandais qui possèdent un téléphone mobile. Les fournisseurs Eircell et Digifone viennent d'expliquer qu'il était tout à fait capable de suivre à la trace un utilisateur et de le repérer à quelques mètres près. Murphy Malachy, responsable du groupe e-droits, explique qu'aujourd'hui la population irlandaise porte efficacement sur elle «un dispositif de marquage». Et en France ?

Very Bad Thing

Le nombre d'infections causées par W32/Badtrans est en train d'atteindre des proportions importantes dans certains pays comme l'Allemagne ou encore le Royaume-Uni. La France s'en sort pas mal : nous avons reçu en un jour sur Zataz.com près de 296 demandes de vaccin. Panda Software vous offre quant à eux l'utilitaire PQREMOVE qui devrait vous soigner de cette plaie.

http://updates.pandasoftware.com/pqremove/pqremove.com

And the winner is...

L'Institut SANS, basé dans le Maryland, vient de sortir la liste des 20 vulnérabilités les plus communes. En tête cette année Microsoft IIS qui est devenu une vraie passoire avec la faille Unicode. Passoire dans la mesure ou votre serveur n'est pas patché bien sûr. La liste inclut les descriptions des vulnérabilités, comment fixer le bug et la description des patches qui peuvent aider à boucher les trous. SANS fait remarquer que les serveurs sous UNIX et Linux sont aussi à contrôler sérieusement.

Le web chiffré

Le piratage informatique coûte de plus en plus cher. Voici le bilan chiffré tiré du dernier colloque cyber criminalité qui s'est tenu en Hongrie ce week-end. Les pertes occasionnées par le piratage de logiciel s'élèvent à 991 millions de dollars, rien que pour les USA. Les escroqueries à la carte de crédit auraient coûté plus de 400 millions de dollars aux banques et à leurs clients en 1999. Les virii informatiques auraient occasionné quant à eux plus de 12 milliards de dollars. Chiffre à prendre avec des pincettes à la vue des soit disant dégâts du virus Kournikova chiffrés à plusieurs millions de dollars et qui en n'auront occasionné à peine quelques dizaines de milliers. Plus dramatique, l'UNICEF annonce que la pédophilie aurait permis aux gros "porcs" d'engranger un C.A. de 3 milliards de dollars rien que chez l'Oncle Sam.

EXEMPLE A SUIVRE

Belgacom propose un audit de sécurité à ses clients abonnés à l'ADSL. Voilà une idée qu'elle est bonne en ces temps où connections illimitées se transforment pour certains consommateurs en gares routières à pirates. Belgacom propose à ses abonnés le test de Scanit, et cela gratuitement. Un test qui examine les failles du système et donne des pistes de solution. A noter que notre navigateur, Navig'scann, vous propose la même chose, mais sous forme de logiciel.

LUTTE ANTI-PEDOPHILES

La police de 19 pays, Australie, Belgique, Canada, Allemagne, Israël, Italie, Japon, Corée du sud, Pays-Bas, Nouvelle-Zélande, Portugal, Russie, Suède, Taiwan, Turquie, Angleterre, France, ont orchestré un coup de filet contre des pédophiles qui opèrent sur internet. Une dizaine de personnes auraient été arrêtées. 130 suspects sont dans le collimateur de la police britannique. Cette opération est le résultat d'une enquête de 10 mois. Ces arrestations font suite à une première rafle en Allemagne le 14 novembre dernier. On ne peut que vous conseiller de visiter le site du Bouclier - www.bouclier.org - pour tenter de lutter contre la pédophilie.

Dcs1000 prend des forces

Cyber Knight, l'un des projets les plus importants visant à optimiser Carnivore, le système de surveillance des communications électroniques utilisé par le FBI, repose sur le développement de logiciels du type de «Magic Lantern». Une fois adressé à un suspect notamment par courrier électronique, Magic Lantern permet de détecter l'utilisation de programmes de cryptage comme le logiciel Pretty Good Privacy, et d'obtenir le mot de passe de l'utilisateur. Ainsi les enquêteurs peuvent suivre tous les messages directement à partir du terminal du seul émetteur. Cette technique de surveillance des communications électroniques permettrait d'éviter quelques-unes unes des difficultés rencontrées par Carnivore. Pour surveiller l'ensemble des communications d'une personne, celui-ci doit en effet également regarder celles de beaucoup d'autres utilisateurs, ce qui a déclenché depuis son lancement un débat houleux aux Etats-Unis quant a la légalité d'un tel système.

actu!

Toute l'actualité du hacking et du piratage !

Planète Underground

SECURITE SOUS MAC

Code511, société d'audit informatique propose, pas le biais de son fondateur "Grungie", un outil de sécurité pour Mac, en Open Source. L'outil se nomme Macintosh Hacker's Workshop. **http://grungie.code511.com/MHW_1.1_Release.sit.bin**

OUPS !

Gibson Research est l'un des références sur le web pour tout ce qui touche à la sécurité informatique. Le problème est que Gibson a désormais mis en ligne un logiciel, plus précisément un scanner de port nommé ShieldsUp, qui pourrait servir à des pirates pour lancer une attaque de Denial of Service à l'encontre d'un site web. La découverte a été présentée fin novembre lors de la session BlackHat d'Amsterdam par *Thor* du groupe HOG.

SECURITE WINDOWS 2000

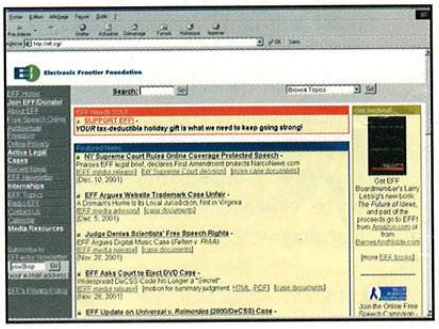
Un bon plan pour ceux qui utilisent le système d'exploitation Windows 2000. Il existe un logiciel qui peut vous aider à configurer votre Windows de manière sécurisée. Vu que Microsoft livre ses produits avec les paramètres par défaut, il n'est pas un luxe de mettre son nez dans les paramètres de sécurité. Linux sera le prochain système à passer à la moulinette. **www.cisecurity.org/sub_form.html**

QUELS COUILLONS !

Les idiots du village sont partout, derniere preuve en date, un spam, courrier publicitaire non sollicité, que nous venons de recevoir. Le fichier reçu comporte pas moins de 500 e-mails de destinataires visibles et en y regardant de plus près on y découvre même une bonne dizaine d'adresses sous forme abuse@...
Détail qui a son importance puisque les e-mails «abuse» servent à se plaindre justement de ce genre de courrier. Les spammeurs se passent eux-même la corde au cou. Vous avez dits idiots ?

Les avocats en tremblent d'avance

The Electronic Frontier Foundation s'attaque à Hollywood. Cette association qui tente d'aider la liberté sur le web vient d'annoncer qu'elle allait rejoindre la défense de Music City, inventeur du système Morpheus utilisé, entre autre, par le logiciel Kazaa. L'EFF veut ainsi faire comprendre à Hollywood que ses tentatives de contrôler les nouvelles technologies doivent cesser. http://www.eff.org



Bidouillez et hackez la XBox !

La nouvelle console de Microsoft **XBox** intéresse de très près hackers et autres bidouilleurs. D'une part l'architecture de la bête est quasiment identique à celle d'un PC et d'autre part sa connexion à Internet peut donc la rendre vulnérable à des intrusions à distance. La voilà à peine sortie cette magnifique console que déjà des groupes de passionnés se sont constitués pour étudier ce qui était possible de faire. Force est d'admettre qu'ils n'ont pas chômé puisque réunis sur le site www.xboxhacker.net, ils ont d'ores et déjà annoncé pouvoir overcloacker la Xbox, déjà cadencée à 733 MHZ ! Mais ce n'est rien face à leurs autres projets qui consistent à dézoner le lecteur DVD de la console et le rendre capable de lire du DIVX. Ultime rêve de ces bidouilleurs talentueux : Rendre les jeux développés sur XBox jouables sur un simple PC. Espérons toutefois que cela reste du domaine du jeu et non du hacking. Je ne me vois pas du tout retourner ma console à la Fnac parce qu'elle a été bousillée par un virus !

AOL fait n'importe quoi

Amusant, le nom de domaine AOL n'était plus la propriété d'American Online depuis le 22 novembre. Ce dernier avait expiré et ne semblait donc plus appartenir au géant US. Le service de presse nous a répondu que «c'était la faute de l'Internic qui met du temps pour mettre sa base à jour». On veut bien le croire à la vue d'un diagramme qui permet de comprendre comment fonctionne le système d'effacement des noms domaines... En général avec Network Solutions, il s'en passe du temps avant que ça soit réellement effacé, facilement jusqu'à plusieurs mois ! On présume donc que pour AOL, la base de données n'a pas été mise à jour, sinon il y a plus de la moitié de la planète qui risque de ne plus pouvoir surfer.
www.snapnames.com/deleteprocess.html

Free.fr a échappé à la catastrophe

La plus grande Mass attaque de France a été évitée de justesse par l'un des plus gros hébergeurs de France : Free.fr . ZATAZ Magazine vous explique comment plusieurs centaines de milliers d'internautes ont failli voir leurs comptes piratés !

Mercredi 30 octobre 2001, la société de services et logiciels de sécurité Internet Security Systems (www.iss.net) faisait paraître sur son site une alerte au sujet d'une nouvelle faille de sécurité découverte par son équipe d'hackers blancs qu'un grand nombre de serveurs étaient vulnérables à l'attaque désormais connue sous le nom barbare de «*SSH CRC32 compensation attack*». Les choses sont devenues beaucoup plus intéressantes lorsque, d'une simple vérification de routine, nous nous sommes aperçus que l'ensemble des serveurs de *proxad.net*, alias *Free.fr*, étaient vulnérables à ce grand danger.

Ainsi le principal hébergeur français victime de cette faille aurait pu voir l'ensemble de ses 400.000 sites piratés, surveillés ou voir même entièrement effacés par un pirate en quelque cliques de souris ! La menace était vraiment réelle puisque au moment de notre découverte, tous les serveurs de Free.fr étaient piratables. Il est probable que, si cette attaque avait été effectivement exploitée, nous aurions pu assister au plus grand «*Mass Defacement*» du Net francophone.

Dans l'orage des attaques actuelles, Proxad peut se vanter d'être passé au travers de la tempête. A ce jour, l'ensemble des machines Proxad/Free, une cinquantaine, ont été sécurisées. Merci qui, merci Zataz Magazine !

" Le principal hébergeur français victime de cette faille aurait pu voir l'ensemble de ses 400.000 sites piratés, surveillés ou voir même entièrement effacés par un pirate en quelque cliques de souris "

nommée *X-force*. Ce bug concerne le *Secure Shell*, protocole permettant d'accéder à un serveur de manière sécurisée et chiffrée. Ainsi tout serveur qui par défaut n'ayant pas été corrigé est potentiellement piratable. De quoi faire frémir, voir détruire les plus importants serveurs de la planète !

Curiosité récompensée

Curieux de l'impact qu'une telle menace pouvait avoir sur l'internet français, *ZATAZ Magazine* a mené l'enquête et découvert

Réponse de Free

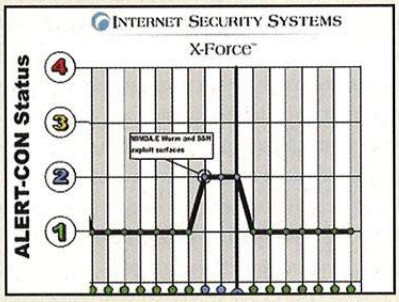
Nous avons posé la question à la direction de FREE. Voici leur réponse : «Cette possibilité de vulnérabilité est connue depuis très longtemps. Nos serveurs, étaient vulnérables, et l'avis de x-force nous a incité à upgradé. Heureusement nous n'avons pas eu de tentatives de piratage. Par prudence suite à l'avis de Info x-force, nous avons mis a jour. Bien cordialement.»

Glossaire

Mass Defacement : Modification par un pirate de plusieurs sites web en même temps.

```
212.27.35.1(perso1-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.2(perso2-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.3(perso3-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.4(perso4-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.5(perso5-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.6(perso6-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.7(perso7-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.8(perso8-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.9(perso9-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.10(perso10-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.11(perso11-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.12(perso12-1.free.fr):22 :SSH-1.5-1.2.27
212.27.35.13(php1-1.free.fr):22 :SSH-1.5-1.2.27
```

La version SSH présentée dans ces fichiers logs de Free nous indique la vulnérabilité de leurs serveurs au moment de notre venue



L'alerte ISS par laquelle tout a commencé !

Focus

Un employé mécontent explique

Un site personnel hébergé chez Wanadoo dénonce le PMU et ses dirigeants. Son auteur proposait en détails toute les techniques pour pirater le système informatique du PMU. Conséquences possibles : des millions de francs de dégats !
Zataz Magazine a enquêté...

« Nous avons piraté lePMU (...) un trésor de 35 milliards de francs vous attend »

A peine arrivés sur le site de cet ex-employé, nous sous sommes drôlement accueillis par une image représentant une femme nue s'intéressant de très près à un cheval, légendée d'un texte qui donne la tournure de ce qui va suivre : «Nous avons piraté le réseau informatique du PMU est nous avons créé ces sites afin de vous faire profiter de nos découvertes. Ci dessous, vous trouverez une documentation complète qui intéressera les hackers. Cliquez ici un trésor de 35 milliards de francs vous attend.» Au dire de l'auteur de cette page les informations données vont permettre d'infiltrer le réseau informatique du Pari Mutuel Urbain. Un acte délictueux qui doit permettre de trafiquer les paris, de faire des virements bancaires ou même de créer des emplois fictifs avec des employés virtuels. Une blague ? Les personnes que nous avons pu joindre au siège du PMU nous ont expliqué que ces informations étaient devenues obsolètes. Pas tant que ça puisque nous avons pu fournir à notre interlocutrice des informations la concernant, disponibles sur le site. Stupeur de la jeune femme, ces informations avaient donc l'air vraies !

Qu'est qu'il y a sur le site ?

On y trouvait des tonnes d'informations, des noms, des téléphones, des fonctions, des mots de passe, des adresses IP. L'objectif de «corbeau» : "Vous donner le plan de l'architecture du réseau PMU avec toutes les informations nécessaires pour que des spécialistes puissent aisément forcer les portes puis pénétrer allègrement jusqu'au réseau PEGASE de manière à pouvoir modifier ou créer des paris. Bien sûr rien ne vous empêche de faire un détour par le réseau interne, par exemple, pour ravager quelques serveurs et postes de travail». Comment ces documents ont-ils pu atterrir sur le web ? L'auteur explique : « Nous avons facilement pu accéder à ces documents ultra-confidentiels que nous nous permettons de vous dévoiler. A la fin de ce document vous trouverez la liste des ingénieurs qui à l'origine les ont conçus pour le PMU.» A la lecture de ces centaines de documents à l'exactitude diabolique, on y trouve des comptes e-mail valides, des noms de personnes salariées et même leurs téléphones. Le rédacteur de ses informations proposait aussi des logiciels permettant de détruire certains serveurs du PMU ou alors, plus dangereux encore, d'avoir accès à toutes les données stockées.

Qu'en penser ?

Notre première réaction a été de prendre cela pour une blague, un hoax. Mais nous avons très vite changé de position devant tant de précision, d'informations techniques et de données sensibles.
Notre enquête nous a ensuite mené sur le forum Emploi de Google sur lequel nous avons pu découvrir des messages d'anciens salariés mécontents eux aussi (voir interview page suivante). Un recommandé a d'ailleurs été envoyé au PMU ainsi qu'au procureur de la République par un certain Sergio Casaretto, ancien du service informatique de la société de paris équestres.

L'objet du délit, le site Internet hébergé chez Wanadoo est aujourd'hui fermé. Il aurait été accessible sur le Web pendant près de deux mois. Force est donc de pouvoir spéculer que nombre de pirates sont désormais en possession de ces informations des plus sensibles...

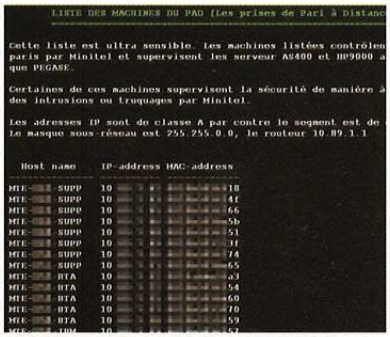
comment pirater le site du PMU

LES PASSES PARTOUTS

Nom du compte	Mot de passe	Groupe	DOMAINE
Administrateur		Administrateurs local	
Administrateur		Administrateurs local	
X011528		Administrateurs local	
SNAARMTH		Admins du domaine	
SQLAGNTH		Admins du domaine	
ALERTE		Admins du domaine	
ARCSERVE		Admins du domaine	
REPLICATOR		Admins du domaine	
PLANNING		Admins du domaine	
DOWNLOAD		Admins du domaine	
USEROPE1	useropel	Utilisa du domaine	

LISTE DES COMPTES UTILISATEURS SENSIBLES

Compte	Nom utilisateur
P090851	YLVIE
P090852	EHENEUC BRUNO
P090853	E VALERIE
P090854	BERTBIE MICHEL
P090855	CHRISTIAN
P090856	DAVID
P090857	ORINNE
P090858	HALIE
P090859	ATRICIA
P090860	ZI CHRISTINE
P090861	NDRE
P090862	ENE
P090863	NE SOLANGE maternité
P090864	SANDRINE
P090865	SCAL
P090866	ATHALIE
P090867	CRYSTEL
P090868	RIC
P090869	S HERVE



LISTE DES MACHINES DU PAO (Les prises de Pari à Distanc

Cette liste est ultra sensible. Les machines listées contrôlen
paris par Minitel et supervisent les serveur AS400 et HP9000 a
que PEGASE.

Certaines de ces machines supervisent la sécurité de manière à
des intrusions ou truquages par Minitel.

Les adresses IP sont de classe A par contre le segment est de
Le masque sous-réseau est 255.255.0.0, le routeur 10.89.1.1

Host name	IP-address	MAC-address
MTE SUPP	10	18
MTE SUPP	10	4f
MTE SUPP	10	66
MTE SUPP	10	5b
MTE SUPP	10	51
MTE SUPP	10	3f
MTE SUPP	10	74
MTE SUPP	10	65
MTE HTA	10	a1
MTE HTA	10	54
MTE HTA	10	60
MTE HTA	10	70
MTE HTA	10	59

Voici les informations disponibles, permettant de s'infiltrer sur les serveurs du PMU !

Témoignage

Avec ces informations le PMU n'est pas en danger. IL EST MORT.

Sergio CASARETTO a travaillé pour le PMU de décembre 1997 à janvier 2000. Il s'occupait du Réseau Interne. Le Réseau Interne est l'informatique interne du PMU, bureautique, serveur et réseau interne (LAN/WAN). Nous avons voulu avoir son avis sur ce site virulent.

Qu'elle était votre mission au sein du PMU ?
Ma mission n'était pas précisée et je n'avais pas d'encadrement. D'ailleurs en ce qui me concerne, le PMU et la société qui m'a employé, Urgence Informatique Europe, seront assignée en justice. D'ailleurs je peux attester de la véracité de certaines informations diffusées pour lesquelles j'ai informé le Procureur de la République. Ayant aucun contact avec le PMU et las des pratiques de certains SSII, je me permets de parler librement parce que j'ai rien à craindre. A part témoigner de pratiques illicites au sein du PMU, j'ai absolument rien à avoir avec les personnes qui ont créé ce site et bombardé de mail. En effet au PMU il avait des problèmes. Majoritairement sociaux. Je comprends que des individus se manifestent. Mais il y a des limites. Je condamne la méthode employée.

Que pensez-vous de l'affaire du site du PMU "piratable" ?
Je la condamne. En effet depuis longtemps le PMU mettait en place des plans sociaux. PEGASE était ouvertement accusé. Pour éviter tout disfonctionnement, le PMU externalisait des services entiers. Je pense que le site en question est un moyen de chantage mis au point par un ensemble d'individus internes au PMU. Peut être en partie prestataires. Evidement cela fait peur. Toutes les entreprises sont vulnérables en interne. Avec ce qui c'est passé tout un système entier c'est trouvé fragilisé voir complètement à refaire. Un coup dur pour l'image du PMU.
Je pense que le point le plus important et que cela ait pu se produire dans une totale impunité. Il n'y a aucun moyen de trouver les auteurs. C'est un crime parfait. Ces gens peuvent agir partout sans pouvoir êtres pris. Je pense que dans cette histoire, la faute incombe au PMU. Comment, alors que tout était cloisonné, une ou plusieurs personnes ont pu regrouper tant d'informations sensibles et les sortir hors du PMU ? Mais, dans tous les cas, pour que les Cybers Criminels puissent agir, il faut de la matière première. Or comment ont-il eu accès à ces informations alors que moi-même occupant un poste stratégique, pendant deux ans, j'en n'étais même pas informé ?

Ca ressemble à des informations provenant de salariés mécontent, non ?
Je pense que certainement oui.

Où est le danger des informations qui avaient été diffusée ?
C'est comme si on donnait une bombe atomique en kit avec le manuel de montage et utilisation aux Talibans. Avec ces informations le PMU n'est pas en danger. IL EST MORT.

Le ver est donc dans la pomme ?
Jamais les entreprises envisagent une attaque en interne. Les attaques externes sont mineures, des pages web changés, un serveur qui tombe. Jamais plus loin. Là, le cas du PMU est une véritable école et mérite réfection. Une attaque invisible interne est bien plus destructeur que le pire des ennemis.

Fluxay, l'assassin du web

Il existe sur le web des centaines de logiciels proposant au premier idiot du village de devenir le «haxor», le pirate à la mode. Beaucoup de ses logiciels ne fonctionnent pas, mais en cherchant bien, il y a des petits trésors qui laissent perplexes par leur efficacité. L'un d'eux se nomme Fluxay.

Il scanne les ports...

Détecte les failles

et se met à jour !

Si le logiciel Fluxay existe pourtant depuis bientôt quatre ans, très peu de gens connaissent son existence. Et pour cause, le programme n'était disponible qu'en chinois. Aujourd'hui, c'est enfin une version anglaise qui nous est proposée, toujours développée par un collectif de programmeurs appellés «Assassin». Ce groupe au nom des plus sympathiques s'est rendu célèbre pour le développement de petits programmes pour les plates-formes DOS/Win, comme par un exemple un logiciel exploitant à 100 % les failles Unicode de Windows NT, mais c'est bien Fluxay qui reste leur chef d'oeuvre.

Ce logiciel semble être l'un des outils les plus puissants «d'audit de sécurité». Certains ingénieurs réseaux très exigeants rencontrés lors du salon de la sécurité informatique, (au CNIT La Défense) nous ont même avoué l'utiliser dans leur travail.

Puissant et simple

Apres avoir télécharger Fluxay.exe sur le site www.netxeyes.com, (le programme pèse dans les 10 mégas) un simple double click de souris vous permet de l'installer et voici ce que propose le monstre informatique. Dans le Menu "File" on y découvre un mode nommé " Advanced Scan Wizard ", comprenez un scanneur qui va permettre de trouver une porte ouverte grâce au ports de l'ordinateur surveillé, mais aussi via les fonctions POP3 - FTP - SMTP - IMAP - TELNET - CGI - SQL - IPC - IIS - FINGER - RPC - MISC - PLUGGIN - En gros, la totale pour cette option de recherche qui permet ensuite de tester failles, mots de passe, etc, et donc d'accéder dans la machine que vous voulez attaquer !

Comment ça marche ?

Dans son fonctionnement, vous l'aurez compris, Fluxay est d'une simplicité enfantine. Il se permet même d'afficher en temps réel, dans une petite fenêtre, le résultat de ses découvertes. Cette traque se termine par une jolie page HTML qui récapitule toutes les failles recensées et offre l'exploit en langage C, si ce dernier est accessible. Ce logiciel propose un nombre invraisemblable de fonctions et petits logiciels différents comme un client SQL, un langage requête base de données, donc accès et gestion de base de données et un client de failles unicodes, une version améliorée de Netcat, un outil réseau, etc. Ce logiciel est gratuit mais attention, aucun code source n'est proposé, ce qui pourrait même laisser penser, pourquoi pas, à une récupération d'informations par l'éditeur du programme par le biais d'un «espiongiciel».

Pour finir, rassurez-vous, ce genre de logiciel n'a rien d'illégal, sauf si vous l'utilisez sur un serveur qui ne vous appartient pas et sur lequel vous n'avez pas été invité !

« Ce logiciel semble être l'un des outils les plus puissants d'audit de sécurité »

Inquiétant ?

Fluxay a une autre fonction qui laisse perplexe par son efficacité. Elle se nomme «Pluggin». Comme vous l'aurez compris cette fonction permet de mettre à jour les dernières failles informatiques découvertes. Certains groupes de "hackers" réalisent même en parallèle de leurs développements des exploits d'intrusion spécialement écrits pour le pluggin de Fluxay. Il n'est pas rare d'ailleurs de voir ce logiciel capable d'infiltrer un serveur avant même que la faille soit rendue publique sur des sites tels que SecurityFocus ou BugTraq.

Canal Plus, la chasse est ouverte

Vous êtes des milliers à regarder illégalement Canal Plus, TPS, et Canal Satellite. Si aujourd'hui tout n'est que pop-corn devant un bon film, bières et hot-dogs devant PSG-OM, prenez garde, le retour de baton arrive...

Lens capitale du piratage télévisuel ? C'est en tout cas ce que nous laisse croire les derniers évènements arrivés début décembre. 17 personnes, travaillant pour la plupart dans le secteur informatique se sont fait simultanément réveillés de beau matin par la gendarmerie. Ce vaste coup de filet, préparé de longue date (20 mois), aura permi de mettre la main sur une bande organisée qui trafiquait de fausses cartes de décodeurs Canal Plus, TPS et Canal Satellite. Plus que de simples bidouilleurs inoffensifs, les forces de l'ordre ont interpellé un réseau extrêmement bien organisé dont les agissements auraient rapporté plusieurs centaines de milliers de francs.

Vaste, l'activité de ces "pirates" allait de la fabrication de fausses cartes à puce permettant de décoder les chaînes de télévisions à péages ou encore de puces électroniques permettant de lire des jeux copiés pour Playstation.

Bientôt jugés, les malfaiteurs risquent deux ans de prison et une amende qui peut avoisiner le million de francs. Gageons par ailleurs que Canal Plus profite de cette aubaine pour faire un sacré exemple !

Une aiguille dans une meule de foin

Si cette vague d'arrestation va faire parler d'elle, il reste cependant à préciser que le phénomène est loin d'être enrayé. Nous avons voulu voir s'il était si simple de se procurer une carte d'abonnement. La réponse est oui. En nous rendant sur un des nombreux forums dédiés au piratage de télévision numérique, nous avons rencontré Malik H., un étudiant de 22 ans vivant à Paris. Son truc à lui, le clonage de carte d'abonnement. «J'ai découvert ça chez mes parents en Algérie. Des boutiques spécialisées qui ont pignon sur rue proposent ce genre de produit. Je me suis donc lancé !».

Malik, lui, ne vend pas et reserve seulement ses services à des amis intimes mais nombreux sont ceux qui s'en sont fait un juteux commerce.

La menace vient de loin

Des pays comme la Thaïlande proposent tous des moyens pour pirater des chaînes numériques. Cartes, décodeurs, certains revendeurs proposent même sur une même carte à puce plusieurs abonnements sur des bouquets différents. La Hollande également a très longtemps été une plaque tournante de ce traffic.

On peut d'ailleurs toujours obtenir dans certaines boutiques d'Amsterdam la recharge d'une carte pirate pour toutes les chaînes cryptées de la planète et autres modifications de décodeurs pour un peu moins de 200 francs français.

Le quotidien marocain Al Aswan publiera lui aussi en avril dernier un reportage sur le sujet. Un pirate local s' y exprimait ainsi : «J'ai acheté en France pour 3.000 FF le programme de piratage des cartes à puce pour les démodulateurs de réception numérique. Je procède également désormais à l'importation du matériel de réception par satellite.»

On ne parle plus ici de bidouillage mais bel et bien d'un nouveau commerce parallèle qui représenterait déjà plusieurs millions de dollars.

Case prison

La loi est très claire sur le sujet, le piratage de chaîne numérique est considéré comme une contrefaçon. Utiliser, vendre ou mettre à disposition ce genre de technique peut vous amener à passer devant un juge, vous retrouver avec une belle amende voir une peine de prison. Une loi a même été réalisée sur mesure pour la chaîne Canal Plus qui, avec son service spécialisé, collabore main dans la main avec la police. Les cas d'arrestations se succèdent, surtout depuis quelques mois. Autre nouveauté de taille, CANAL Plus a lancé plusieurs "attaques" numériques à l'encontre des pirates : Lors de la diffusion du film "STARWARS Episode 1" ou encore lors du match de football PSG/OM, la chaîne a envoyé un signal électronique a distance qui a permi d'identifier et détruire les installation pirates.

Le Black Sunday : des milliers de décodeurs pirates détruits à distance

Les responsables des services techniques de Canal Plus, TPS et AB SAT n'ont pas souhaité nous répondre. Tous ce qui touche à la lutte contre le piratage est «Secret défense». Aux USA, la communication y est plus grande, quoique ... La veille du Super Bowl 2001, la finale du championnat de football américain, le diffuseur Direct TV détruira à distance plusieurs dizaine de milliers de décodeurs et cartes pirates. Cette attaque a été appelée par les pirates le «Black Sunday», comprenez le dimanche noir.

DOSSIER EXCLUSIF

MATIGNON PIRATÉ

Jamais de l'histoire du hacking en France une intrusion de telle dimension a été révelée au grand public. Des serveurs de Matignon, plus précisément du service d'information du gouvernement ont reçu la visite d'un hacker de haut-vol. Contacté par le Nouvel Observateur, SVM et d'autres revues prestigieuses, l'hacker Alone Trio nous a fait l'honneur de réserver son histoire exclusivement pour Zataz Magazine. Voici l'itinéraire d'un hacker pas comme les autres, emporté par son talent.

1985, l'année de la révélation

L'Atari ST pointe son nez et la révolution informatique débarque chez le particulier à grands renforts de publicité. Antoine, qui se fera appeler AloneTrio, aura une révélation grâce à cette machine.

Comme pour beaucoup d'utilisateurs, cette passion se met en place lorsqu'il a dans les mains la première disquette d'un jeu piraté. AloneTrio s'en souvient encore : «Sur l'écran, une phrase : Cracked By *Blade Runner*. C'est là que je me suis dit, c'est ça que je veux faire !» Il va donc commencer à tâtonner, chercher, fouiner. Dans l'une des intros pirates d'un de ses jeux, il découvre, cachée entre des lignes de programme, une adresse d'un serveur minitel nommé RTEL. Ni une, ni deux, il s'y connecte et y passera des heures, des jours et des nuits à discuter, échanger des trucs et astuces, des idées avec d'autres passionnés du piratage. Très vite son talent est mis en avant, il entre dans la «Scène Démo» dans laquelle il deviendra un «Elite», un pro qui signera ses créations sous le pseudo ALONE. Coté école rien à faire, il restera toute sa scolarité dans le fond de la classe. «Je n'avais rien à y faire, car de toute façon on y apprenait pas l'assembleur. Moi je voulais coder, coder et encore coder» .

L'année Minitel

Sur Rtel, il rencontre *Dr Cyber*, son premier gourou qui l'incite à rejoindre un serveur minitel de pros du piratage nommé E.F.Z., *European Free Zone*, hébergé sans le savoir à l'époque par le 3615 talk.

Pour ceux qui ont connu E.F.Z., on y apprenait beaucoup de choses sur le hacking et le phreaking. On pouvait d'ailleurs y rencontrer des informaticiens qui sont aujourd'hui devenus de véritables mythes, comme *Neuralien*, créateur du magazine électronique underground *Noway* ou encore des pointures du piratage de jeu comme le groupe *Paradox*. «C'est là que je découvre aussi des techniques qui permettaient de ne pas payer le téléphone, comme la technique *Bleu BOX* par exemple. Je trouvais ça extraordinaire.»

Côté diplôme, Antoine s'accroche tant bien que mal et décroche un BEP électronique, un CAP avec mention, un BAC Pro maintenance des réseaux bureautiques et télématique. Il débutera un BTS en informatique industrielle, mais ça ne lui donne toujours pas le goût des études : «Là aussi ce fût pénible pour moi. Jouer avec des capteurs, des machins via le port série. Moi je voulais faire de la 3D, du full screen, du plasma, de la démo !» C'est un stage dans une web agency qui va lui mettre définitivement la main au web.

A la fin du stage on lui dit : «toi t'es fort, on te veut», il n'est pourtant

Alonetrio, un hacker brillant qui a infiltré Matignon...

...et qui attend maintenant son jugement.

qu'en première année de BTS. «On me dit que ce n'est pas grave, que je dois quitter l'école (...) Je réfléchis, c'est peut être la chance de ma vie et je signe mon premier contrat». Il commence à chercher, fouiner et surtout apprendre. Sa première découverte se fera sur le jeu *Tetrinet*, un serveur de jeux en ligne copiant le principe du célèbre Tetris. «Je sniffe ce qui est envoyé par le serveur durant une partie, décortique et comprends le protocole, je programme un faux serveur qui réplique parfaitement le comportement du jeu original à la différence près que j'ai rajouté des petites fonctions de triche !». *AloneTrio* fera parti des meilleurs joueurs sur *Tetrinet*. «Ah les pauvres, s'ils savaient !» nous confiera-t-il.

Du jeu au hacking

Tetrinet ? Du gateau pour ce bidouilleur. Il retente le coup sur un autre serveur, plus gros, plus important, plus difficile. Sa cible, le site *Milkado*, qui propose un jeu en flash, une sorte de jackpot.
Là il relance sa machine intellectuelle, analyse et «Qu'elle ne fût pas ma surprise de m'apercevoir que la décision de gagner ou de perdre était gérée du côté client». Antoine va essayer de créer lui-même un paquet ip contenant des valeurs gagnantes. Résultat, le serveur lui répond bravo et gagne dans la foulée un chèque de 50 Francs. «Je décide de ne pas l'encaisser et je les contacte par e-mail afin de les avertir de la simplicité de les pirater».
Comme malheureusement dans beaucoup de cas, il ne recevra aucune réponse. Bizarrement les principales failles seront corrigées le jour même. «C'est d'ailleurs la première fois que je commence à regretter d'avoir aider des gens aussi ingrats». Une première déception....

Quelques semaines plus tard il va refaire le coup sur le site d'une grande marque de charcuterie *Bordeau Chesnel*. Cette société offre une BMW Z3. Le concours est simple, un jeu de l'oie avec des tirages de dés aléatoires et des points à accumuler. «Je joue plusieurs parties normalement afin de comprendre le mécanisme et à chaque fois je fais environs 3 000 points. Je trouve une petite astuce pour pouvoir obtenir le score de mon choix, la Z3 me fait quand même pas mal rêver alors je finis par craquer et m'inscrits avec, attention : 546.548.612 points ! "

« je découvre qu'il est possible de prendre la main sur n'importe quel nom de domaine »

Avec son score faramineux et les 3.000 points qu'un joueur normal ne peut pas dépasser, il n'y a aucun doute, *Alone* pense qu'il va se faire attraper. Un mois passe et le jour des résultats arrive. Une belle surprise pour le bidouilleur. Il n'est pas le gagnant. Le vainqueur de ce jeu avait engrangé à peu près dix mille fois plus de points ! De quoi se faire une belle indigestion de rillettes ! *Alone* enverra un courrier aux organisateurs de ce jeu mais personne ne lui répondra. Encore un soufflet...

De la déception au contrôle

Une autre histoire aurait pu transformer ce hacker en un cyber-escroc. «J'ai un jour déposé un nom de domaine que j'avais acheté chez *Network solutions*, mais lors de mon dépôt j'avais par habitude mis les coordonnées de ma société. Alors j'utilise le formulaire du site de la NSI pour modifier les coordon-

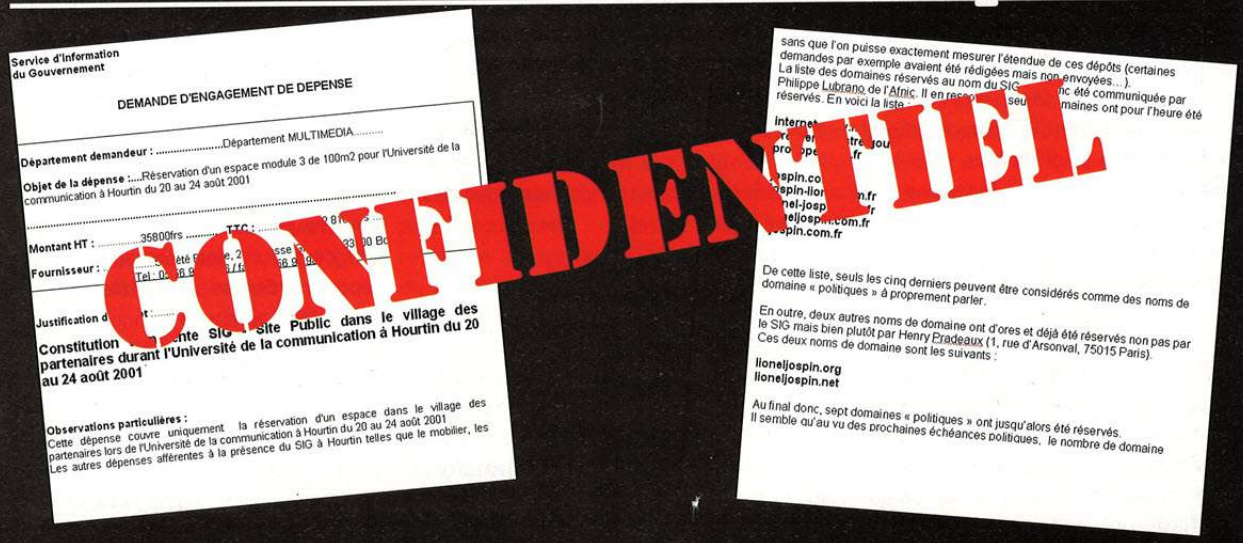
DOSSIER EXCLUSIF

nées, qui envoit un e-mail de demande de confirmation à ma société . C'est là où je découvre qu'il est possible de prendre la main sur n'importe quel nom de domaine». Une faille qui permet ensuite de modifier les DNS et ainsi faire pointer l'adresse détournée vers n'importe quel autre site. «J'envoie l'info à quelques-uns un de mes contacts. Ma surprise fût grande de lire quelques jours après dans les news de *Yahoo!* que c'était un gars de chez France Télécom qui avait trouvé l'astuce. Cette personne faisait partie de mes correspondants." Troisième déconvenue.

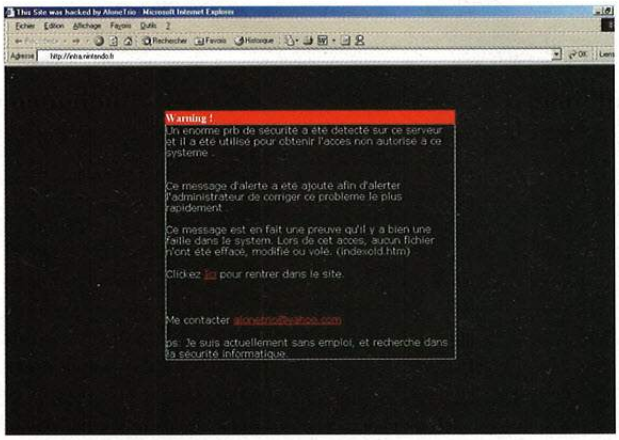
La Web Agency où il travaille finit par déposer le bilan. Elle est rachetée et on propose à *AloneTrio* une formation en sécurité informatique. «Un vrai changement de profession pour moi, car je suis devenu responsable sécurité d'un très grand nombre de machines, sur une architecture assez conséquente.»
Pendant des jours et des nuits il pratique son métier avec passion. Regarde des alertes, lis des kilomètres de logs et de mailing-lists dédiées à la sécurité, chate sur irc dans les canaux tendancieux et, son plaisir suprême, fait des tests d'intrusions pour le compte de son entreprise.
L'une de ses premières grosses découvertes date du début de l'année 2001. Il traque, pour le compte de son entreprise, les failles unicodes. Lors d'une vérification de routine, il se rend compte qu'un groupe de pirate appelé PoizonBox a infiltré les serveurs qu'il surveille. En cherchant un peu, *AloneTrio* découvre que l'un des serveurs hébergeant **Caramail**, un poste de développement, a lui aussi été infiltré par le même groupe de pirates.
Plus grave, *Alonetrio* s'aperçoit que ce poste héberge en plus les informations de tous les comptes clients de Caramail laissés sur ce poste par négligence d'un des techniciens de Caramail. Tous les logins et mots de passe de Caramail sont à la portée de n'importe quel pirate débrouillard !
«Je m'empresse d'écrire à l'adresse admin@caramail.com qui ne me répond pas. Dans le doute je m'adresse au contact technique de caramail.com, un certain cs@caramail.com à qui j'écris. La réponse ne se fera pas attendre et ce soir là nous n'étions pas loin du champagne.»
Puis la nouvelle tombe, la société qui emploi *AloneTrio* traverse une grosse crise et va devoir à nouveau déposer le bilan.
Il fait maintenant partie des licenciés. «Là je me suis dit : Et si je continuais à faire ce que je faisais, mais en spécifiant que je suis à la recherche d'un

> «Tous les logins et mots de passe de Caramail sont à la portée de n'importe quel pirate»

Les documents interceptés



Outre les dizaines de logins et mots de passe appartenant à des membres du gouvernement, ce sont également des messages qui ont été interceptés. Ici deux lettres échangées traitant des noms de domaine à déposer pour les futures présidentielles. Curieux, ils savaient déjà que Jospin étaient candidat ? :-)



Voici à gauche à quoi ressemble l'Intranet de Matignon et, à droite, la petite visite par AloneTrio chez Nintendo. Nous aurions pu vous en montrer plus, mais là, nous aurions été dans l'illégalité !

emploi, je justifierai mon savoir-faire non pas par mon CV mais par des faits concrets !». C'est à ce moment *qu'AloneTrio* prend le dessus sur Antoine. «J'ai commencé à perdre un peu les pédales (...) Je me dis que si mes correspondants ne lisaient pas les e-mails que j'envoyai, j'irai carrément remplacer la page d'accueil de leur site.»
Quelques piratages plus loin, le projet emploi d'*AloneTrio* ne fonctionne pas. Antoine reprend le dessus et contacte les administrateurs de **Nintendo** et du magazine **Transfert**, chez qui il découvre des failles de sécurité. «Les entreprises me contactaient très régulièrement afin de me demander mon CV et éventuellement me proposer un emploi», mais jamais aucune suite ne lui sera donnée.

Le pseudonyme *AloneTrio* commence à remonter de plus en plus dans les moteurs de recherches, de part, entre autre les nombreux *défacements* qu'il a pu effectuer et que l'on retrouve sur des sites miroirs. A la suite de ses exploits de nombreux groupes de pirates vont le contacter pour le recruter, ou pour participer à des frappes informatiques, soit disant politiques. «J'ai eu de tout, du groupe de *Script Kiddies* au groupe de fous avec des idées politiques de dingue». Il refusera toutes les propositions, il ne veut pas devenir un pirate, juste trouver un emploi.

D'un Ministère à l'autre

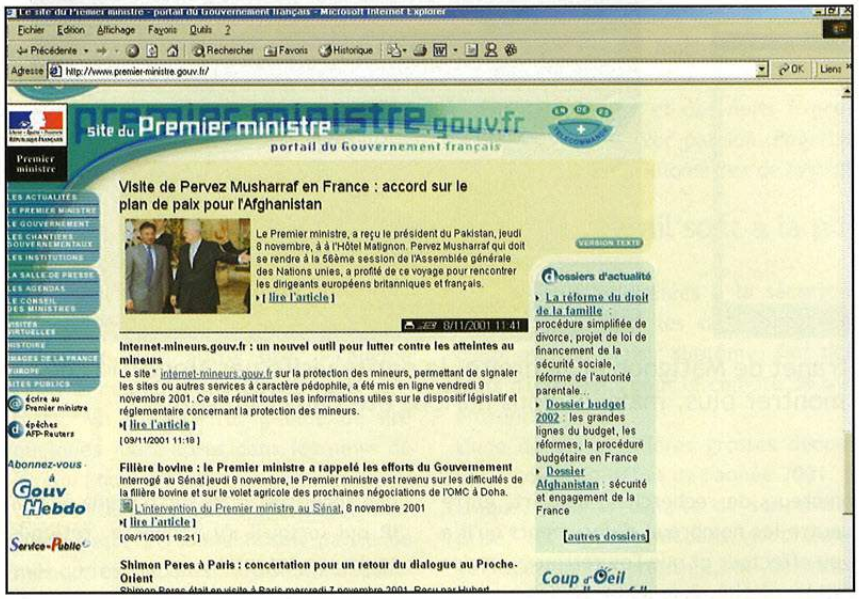
En septembre, Antoine et son amie regardent à la télévision le spectacle de **Jean-marie Bigard**. A la fin de l'émission il aperçoit l'adresse du site internet de l'artiste. Par jeu, et par curiosité, il cherche des informations et failles de sécurité autour des adresses ip du site de Bigard. Il trouve des dizaines de sites non sécurisés, mais surtout une adresse IP qui lorsqu'il s'y connecte, retiendra toute son attention.
Un message apparait : « Bienvenue sur le site du SIG. Service d'Information du Gouvernement. Login / Password.» Un brin de panique s'installe. Le SIG est tout de même la cellule de communication de **Matignon**. Toutes les correspondances destinées au gouvernement y transitent.

La curiosité est un vilain défaut, et le danger est grand mais à ce niveau là, *AloneTrio* n'a qu'une chose en tête, trouver un emploi et donc se faire remarquer. Il étudie de plus près le serveur et découvre une base de données nommée SIG.mdb de 60 Mo. «Là j'ai été pris de panique. Je me suis dit, je fais quoi ? Je les appelle ? Mais bon, si c'est une base fictive mise là pour des simulations, je vais avoir l'air malin,

Service d'Information du Gouvernement

AloneTrio est la partie visible de l'iceberg mais a-t-il était l'unique visiteur ? Il a prévenu les intéressés de son intrusion. Mais n'y a-t-il pas eu d'autres curieux aux intentions nettement moins constructives que celles de ce hacker ? Des voyous qui ont pu intercepter e-mails, bases de données, photos ? Détourner et, qui sait, revendre des documents sensibles, comme par exemple, l'audit de sécurité informatique des serveurs de Matignon ou encore cette " note d'information " sur les noms de domaines liés à Lionel Jospin et à la présidentielle de 2002. Au Service d'Information du Gouvernement on se veut rassurant : La faille a été bouchée, point final. Quant à savoir si des informations confidentielles circulent désormais sur Internet, cela n'intéresse apparemment pas les techniciens du SIG qui préfèrent faire oublier leur maladresse !

DOSSIER EXCLUSIF



surtout aux vues de la façon dont elle est protégée». Alonetrio se lance et télécharge cette base pour s'en assurer, qui, il le découvre rapidement, n'est pas si anodine. De nombreuses informations sensibles y sont stockées, avec logins, mots de passe, adresses e-mails de dizaines de personnes du gouvernement français, d'ambassades. « Là je me dis qu'il y a un vrai problème et que le SIG a vraiment besoin de quelqu'un comme moi». Il utilise alors un mot de passe par hasard pour le tester sur le serveur, et là, stupeur, il vient d'être connecté à l'Intranet de Matignon !

Aux mains d'un criminel, l'Intranet du gouvernement aurait pu être pillé, détourné, bref, une catastrophe qui aurait eu des répercussions au niveau international.

Premier reflexe tout à son honneur, Il envoit un e-mail à Matignon prévenant de sa découverte et en profite pour signaler qu'il recherche un emploi.

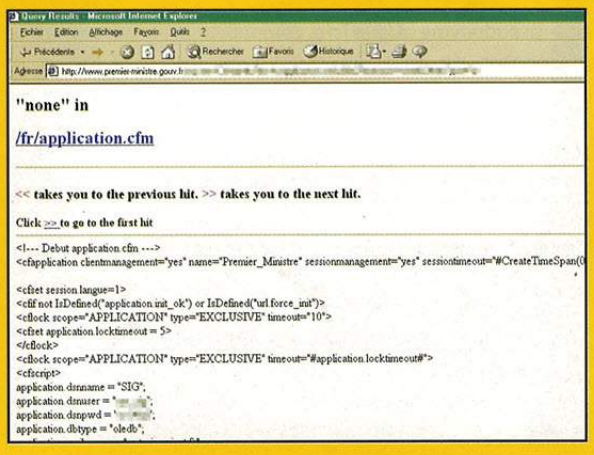
La réponse ne se fera pas attendre : « Monsieur, Comment puis-je vous joindre ? Pouvez vous m'appeler ? Je vous remercie, Cordialement, Benoît T.» *AloneTrio* se dépêche, il y a peut être un travail à la clé. «Je prépare alors un papier regroupant mes informations concernant les machines de Matignon.»

S'enchaînent alors plusieurs coups de téléphone où curieusement, l'étonnement et la gratitude de son correspondant au SIG fait place à un certain malaise voir de l'animosité. Quelques jours plus tard, c'est la police qui sonnera à la porte d'*AloneTrio*. Cette fois, ce n'est même plus de l'ingratitude, Alonetrio s'est fait piegé pour avoir tenté de rendre service au gouvernement.

La police judiciaire et le nouvel *Office de police Informatique* souhaitent l'entendre. «L'ambiance est plutôt détendue. Ils ont compris que je n'étais pas un bandit. Les policiers de l'office

Le site de Matignon et les mots de passe

Ce n'est pas la première fois que le site de Matignon risque de se faire pirater. Au mois de mars 2001, *ZATAZ Magazine*, mais aussi le magazine *Transfert*, découvrent une faille sur le site du Premier Ministre. Le site tourne sous IIS 4 et «bénéficiait» d'une faille due à l'utilisation de fichiers .htw par Index Server et IIS. En fait le problème provenait du fichier null.htw qui agissait ici comme un pointeur et permettait de visualiser la source des fichiers sur le serveur. Grossièrement un pirate et quelques manipulations avec les pages ASP, ce dernier pouvait avoir accès au login et mot de passe. Il aurait pu placer sur le site n'importe quelle information de son cru. Imaginez un pirate parlant au nom du Premier Ministre sur un boycotte des produits Danone ou bien, beaucoup plus drôle, un Mea Culpa de Jospin de toutes les boulettes du gouvernement. Ah...ça fait rêver !



Les ministères finlandais, italiens et portugais aussi !

Pour avoir une idée du reste de l'Europe, nous avons suivi les liens que proposent le site premier-ministre.gouv.fr. Bilan, les autres ministères européens avaient quelques problèmes du même ordre. Le site du Gouvernement finlandais et de son Premier ministre. En quelques clics, la biographie, les discours et les communiqués des ministres. On s'aperçoit également en quelques clics que ce site est victime du même problème que le site du gouvernement français. En utilisant la faille ASP, de la même façon, on pouvait obtenir les sources des pages dynamiques et en quelques requêtes le global.asa et ses informations apparaissaient. Même punition sur le site italien, Portugais. Ce genre de faille se patche chez Microsoft, et cela gratuitement.
www.microsoft.com/technet/security/bulletin/ms00-006.asp

fouillent mes disques durs. Une perquisition numérique qui va durer un peu plus de 3 heures. Le lendemain on m'explique que c'est le SIG qui a porté plainte pour "Intrusion dans un Système de Traitement Automatisé de Données"» Autre surprise qui n'est plus qu'un détail qu'autre chose, une autre des sociétés qu'aurait piraté *AloneTrio*, **Infoclar**, a, elle aussi, porté plainte dans la foulée. La fiancée du prévenu sera elle aussi interrogée plus de quatre heures. «Elle qui a du mal à trouver le bloc note dans un PC !». Heureusement, le procureur acceptera sa libération à la demande d'Antoine, qui préfère oublier son pseudonyme d'*Alonetrio*. Lui par contre sera l'objet de toutes les attentions des policiers qui l'écouteront durant 23 heures de garde à vue enfermé «avec des voleurs et des alcooliques en train de cuver . Maisles policiers ont été très sympas. Ils m'ont même refilé, sur CDROM, mes sites que j'hébergeais car ils ne pouvaient pas me rendre mes disques durs pour le moment.»

Et maintenant ?

Aujourd'hui Antoine attend son jugement. Il a tiré un trait définitif sur le Hacking, mais surtout sur la capacité des gens à comprendre que ses intrusions n'étaient pas le fait de volonté de nuire mais bien d'aider la communauté informatique, et pourquoi pas trouver un bon emploi à la mesure de ses talents. Est-ce là un crime ? La loi française répond par l'affirmative. Il conviendrait cependant de relativiser et d'espérer que les instances juridiques relaxeront ce hacker déchu.

Hacker brillant cherche emploi stable

Antoine, Alias AloneTrio, c'est toujours retrouvé face à des ordinateurs, il faut dire aussi que son père est un ingénieur en informatique. Très jeune il va côtoyer de gros calculateurs à bandes, ceux avec deux gros cercles qui tournent dans touts les sens. Son jeu à l'époque, taper sur le clavier de la machine à perforer les cartes afin d'obtenir le maximum de confettis. En 24 ans il aura connu les ordinateurs SORD, Lynx, Sega 3000 Yeno, Atari ST, Amiga, PC. Antoine recherche toujours un emploi et nous serions très content s'il pouvait en trouver un à la hauteur de ses talents . Pour le contacter, écrivez à la rédaction de Zataz Magazine qui transmettra.
courrier@zataz.com

ENQUÊTE ZATAZ

Fausses cartes bancaires

le fléau

Depuis plusieurs mois la rumeur est persistante, un logiciel serait capable de cloner, de manière industrielle, des cartes bancaires. Vrai ou faux, la rumeur s'est propagée à la vitesse grand V et commence à intéresser les bidouilleurs, mais aussi, les criminels. Etat des lieux du piratage des cartes bancaires.

Compte et décompte

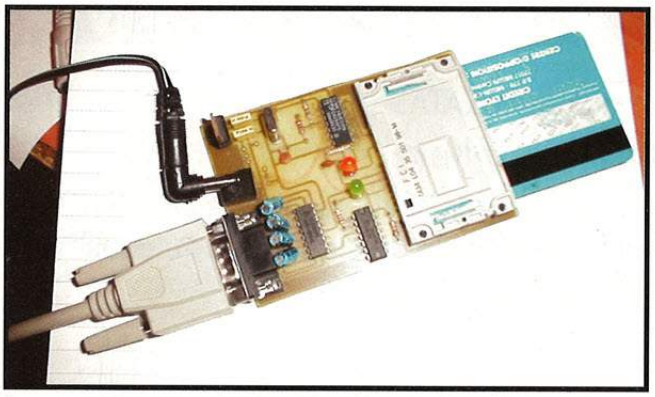
Avant l'apparition du logiciel Gezerolee la fraude bancaire sur Internet se limitait, façon de parler, au détournement d'informations inscrites sur les cartes bancaires ou à l'utilisation de générateur de numéros. Le logiciel Gezerolee que l'on trouve sur le réseau en trois cliques de souris est une véritable bombe à retardement car son utilisation est d'une simplicité... comment dire... dramatique. Ce programme contient un ensemble d'outils destinés à procéder à quelques expérimentations sur une carte bancaire. Avec cette boîte à outils, il est possible de lire et de décoder complètement les informations d'une carte bancaire, comme l'historique de ses transactions (après saisie du code confidentiel), d'intercepter et d'analyser la communication entre la carte et un lecteur (lecteur universel de cartes à puce), d'envoyer des commandes ISO à la carte et d'en analyser le résultat et, dans une certaine mesure, de créer une "copie personnalisée" de sa propre carte (copie totale pour les données, et partielle pour les instructions). L'auteur du logiciel, inconnu à ce jour, explique ainsi la raison d'être de ce programme: " Pouvoir enfin connaître le contenu de sa carte bancaire (après chaque transactions par exemple, pour gérer ses comptes, en suivant le relevé intégré à la carte), et d'autre part, être capable de réaliser un émulateur de sa carte bancaire, capable de "leurrer" un lecteur universel de carte à puce ".

Yescard, kesako ?

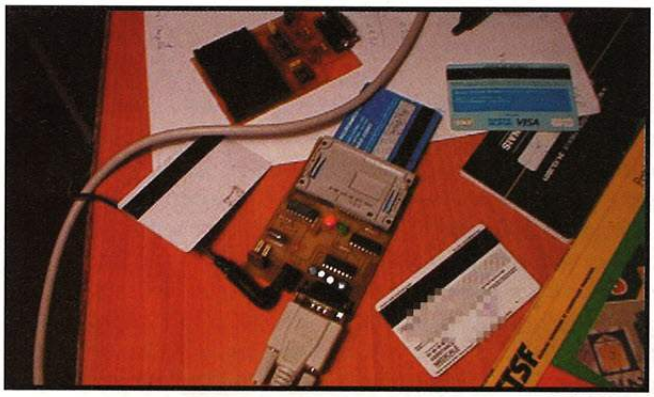
Une Yescard est un simulacre de carte bancaire dont la puce fonctionne et est reconnue par les terminaux de paiement électronique. Attention, nous ne parlons pas du piratage de la bande magnétique, mais bien de la puce, et ce quel que soit le code à quatre chiffres utilisé par la carte pour valider les transactions. Gezerolee a donc bien sûr été pris très au sérieux par le GIE carte bleue qui a mis les bouchées doubles en novembre et décembre pour tenter de contrer les contrefacteurs. Il faut savoir que le système actuel permet de détecter l'utilisation d'une Yescard sur un terminal en à peu près vingt-quatre heures, délai assez long pour réaliser un flagrant délit !. Le mieux en matière de protection, dixit Laurent Pelé, ingénieur passionné du sujet, serait une authentification dynamique entre le terminal de paiement et la puce. Conversation chiffrée, cela va de soit.

Quel risque ?

La prochain texte, loi sur la sécurité quotidienne, va promettre une sanction exemplaire aux contrefacteurs, mais aussi aux bidouilleurs trop curieux. La punition est de taille, sept ans d'emprisonnement et



Nous ne faisons pas qu'en parler. Nous avons pu assister à des démonstrations édifiantes !



750.000 F d'amende. La loi est très claire, et considère une fraude à la carte bancaire comme " le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre une fraude à la carte bancaire ".
Difficile pourtant de faire la différence entre des techniciens passionnés qui peuvent aider à sécuriser les systèmes comme Serge Humpich par exemple et des criminels prêts à se faire de l'argent à bon compte !

Et maintenant ?

En France, les arrestations se succèdent déjà.. Deux pirates de cartes bleues ont été arrêté dans la banlieue de Dunkerque, dans le nord de la France. Les deux hommes originaires de Grande-Synthe ont été pris la main dans le sac au moment ou ils se servaient de l'essence dans une pompe à essence de la ville. La police aurait pour le moment dans ses petits papiers pas moins de 600 opérations frauduleuses sur toute la région dunkerquoise, ainsi qu'en Belgique. Le préjudice n'est pas encore chiffré mais pour la seule station service utilisée par ces escrocs, le montant des pertes avoisinent les 150.000 FF.
Dans un autre style, début novembre, un ingénieur en informatique de 26 ans s'est fait pincé par un patron de vidéo club chez qui le " pirate " faisait ses courses avec de fausses cartes bancaires (voir nos brèves).

la suite page suivante

Des informations sur Internet

Nous ne vous présenterons pas ici des adresses au contenu illégal. Toutefois, vous pourrez trouver de la documentation sur les Yescards sur le site de Laurent Pelé www.parodie.com et sur ce forum privé : http://pub79.ezboard.com/fyescardfrm23

ENQUÊTE ZATAZ

Témoignage

Laurent Pelé est le webmaster du site parodie, mais aussi l'un des premiers à avoir suivi l'affaire de Serge Humpich, l'ingénieur qui a découvert une faille dans les CB. M. Pelé fait parti des experts qui étudient la mouvance Yescard.

Qu'elle est l'évolution de la sécurité des CB ?

Les cartes bancaires en elles-mêmes n'ont pas évolué depuis novembre 1999 où elles ont subi une modification plus d'ordre marketing que technique : ajout d'une clé 768 bits, mais la clé 320 bits cassés depuis 1998 par Serge Humpich subsiste et peut donc toujours être utilisée pour les cartes bancaires (Yescard). De plus il reste possible de cloner une carte bancaire à puce sans avoir besoin du code secret. La puce est utilisée par les banques comme un gadget : toutes les informations nécessaires au clonage de la puce sont accessibles sans le code secret, et les capacités de calcul de la puce ne sont pas exploitées.

Les terminaux des commerçants ont été changés, bon signe ?

Les banques ont changé légèrement les terminaux de paiement, alors que le problème à la base est dans le protocole d'authentification de la carte, pas les terminaux de paiement. Pourquoi ont elles changé les terminaux de paiement : parce que la modification n'est pas à leur frais mais celui des commerçants et elles voulaient forcer les commerçants à passer à l'Euro (les cartes n'ont même pas été adaptées pour l'Euro et comportent des bugs dont sont déjà victimes les porteurs) puis à EMV (pas plus sûr mais américain). Les banques ont réussi la prouesse de faire en sorte que ceux qui payent les commissions (les commerçants) soient également ceux qui investissent ! Et les banques n'ont pas mis un sou pour la sécurisation, pourquoi le ferait-elle ? Plus il y a de fraudes, plus elles touchent de commission. Concernant Internet et la vente à distance, elles n'assument pas le risque mais touchent des commissions doubles sur les transactions frauduleuses !

Les modifications des TPE sont pitoyables, les Hackers ne comprenaient pas pourquoi leur Yescard ne fonctionnaient pas sur un TPE, ils ont loggé une transaction samedi dernier et le samedi soir figurait sur Internet le log commenté qui expliquait les "verrous additionnels" mis en place par le GIE CB et les moyens de les contourner. Cela m'a bien fait marrer.

La sécurisation est en cours ?

Les CB ne sont absolument pas en cours de sécurisation. Le dernier replâtrage date de novembre 1999 mais comme il y a une compatibilité ascendante : Toutes les failles découvertes fonctionnent encore et plus ça va plus on trouve de failles. Il faudrait abandonner tout le passif et repartir sur de bonnes bases, A mon avis, un produit concurrent tel que le porte-monnaie électronique pour échanger de l'argent de porteur à porteur peut émerger car cela requiert très peu d'investissement (terminaux à 250 francs) et cela respecte la vie privée. Je ne crois pas, à court terme, aux solutions de paiement limitées à Internet, elles ne sont pas viables financièrement (marché trop faible actuellement et le problème est aussi du côté de la confiance envers la vente à distance).

Mission : se procurer une Yescard !

Nous avons voulu savoir s'il était si simple de se procurer un Yescard. Notre recherche a débuté sur le web, dans l'un des nombreux forums traitant du sujet. Contact froid au début, notre enquête s'annonçait plutôt mal. Quelques jours et contacts plus tard, nous en savons tellement que nous pourrions, nous même, la fabriquer cette fameuse carte. Pour cela on nous propose le matos complet pour faire des yescard pour la modique somme de 300 FF. Des boutiques parisiennes proposent, elles, un matériel pour quelques centaines de francs supplémentaires. Nous nous sommes mis dans la peau d'un petit voleur, nous notre but était donc d'acheter une carte. Le Matériel existe, là on en est sur. Certains rassemblement de " hackers " parisiens s'en sont d'ailleurs fait une spécialité. Notre quête continue, une prise de contacte est effectuée et nous rencontrons un " bidouilleur " sur le parvis du CNIT. Pour 500 FF nous achetons une carte en plastique de couleur or qui arbore une puce. Transaction terminée, nous avons testé le clone de CB (NDR, avec l'autorisation des propriétaires des magasins) sur les terminaux de boutique de location de films vidéo. Bilan, cela marche très bien. Nous aurions pu rentabiliser cette carte dans l'heure si nous avions été l'un de ses nombreux utilisateurs de Yescard.

Sites utiles

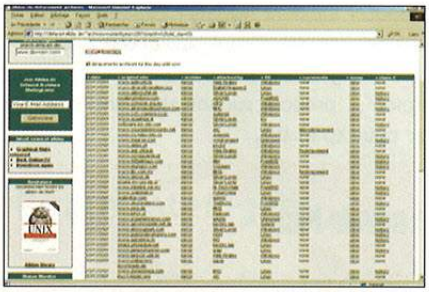
Dans chaque numéro de ZATAZ Magazine nous allons faire le tour des sites internet les plus utiles dédiés à la sécurité informatique. Sites français ou anglais, vous aurez de quoi vous faire un petit carnet d'adresses des plus utiles !

Une si jolie loi

Le site LSIJolie n'est pas au premier abord un site dédié à la sécurité informatique, mais plutôt à notre sécurité de citoyen. Ce site décortique la future loi, loi sur la société de l´information, et démontre que cette dernière a été conçue d'une étrange manière. News, forums et pétitions vous permettront de vous faire une idée du sujet.

Langue : Français
Url : www.lsijolie.net
Logiciels disponibles : non
Autre site du même type : eff.org

AllDas



Ce site allemand est devenu la nouvelle référence des miroirs de sites piratés. Ce site référence, dans la mesure ou les administrateurs sont prévenus, les piratages qui touchent les sites web. Fonctionnement simple et complet. Le site classe par jour, mois et années les piratages en proposant le lien direct au site touché par un pirate, la capture du piratage mais aussi la faille employée. Alldas remplace le site ATTRITION qui proposait ce même type d'information depuis 1998.

Langue : Anglais
Url : www.alldas.de
Logiciels disponibles : non
Autre site du même type : www.attrition.org

Ciac

Ce site n'a pas pour but d'être joli. De l'information, rien que de l'information dédiée à la sécurité informatique. Le Computer Incident Advisory Capability est une agence américaine qui a, entre autre, mis la main sur l'un des mouchards informatiques du dernier-né de Microsoft, Windows XP. Le site, austère, permet de trouver très rapidement les dernières informations sur comment protéger son OS préféré.

Langue : Anglais
Url : www.ciac.org/ciac
Logiciels disponibles : oui
Autre site du même type : www.first.org

Security Zoom

Ce site en français lancé en l'an 2000 est classé par thème. Windows ou Linux, vous y trouverez les derniers patches qui protégeront votre machine ainsi que quelques articles sur comment installer un serveur Linux, apache, ... Le surf y est simple, coloré et rapide. Vous y trouverez aussi des rubriques sur comment vous protéger sous ICQ ou encore en chattant sur l'IRC.

Langue : Français
Url : www.security-zoom.com
Logiciels disponibles : non
Autre site du même type : www.secutest.org

Hackito

Le portail Hackito propose un ensemble de site web dédié à la sécurité informatique, à l'underground, aux virii (Pluriels de virus). Classés par thèmes, gratuits ou commerciaux, Hackito vous offre en quelques clicks un bon aperçu de ce qui existe en ce moment sur le réseau. Petit plus, vous pouvez inscrire votre propre site internet qui sera du même coup référencé dans ce portail.

Langue : Français
Url : www.hackito.org
Logiciels disponibles : oui
Autre site du même type : www.astalavista.com

Enlever les mouchards de Windows

Microsoft nous aime, c'est bien connu. Il nous aime tellement qu'il a placé dans certains de ses logiciels de petites fonctions un peu trop curieuses. Exemple avec la famille Windows.

Les mouchards

Microsoft a introduit dans Windows 98 un système d'identification des utilisateurs plus vicieux que celui de Intel placé dans ses premiers Pentium III et Xeon III. Alors qu'Intel annonçait ouvertement l'existence de son PSN (Processor Serial Number), Microsoft avait tenu secrète l'existence de son Guid (Globally Unique Identifier ou identificateur global unique). C'est au début de 1999 que son existence a été révélé par un développeur américain, puis confirmée par Microsoft.

L'assistant d'enregistrement de Windows 98 vous affecte un code identificateur exclusif qui identifie votre PC. A l'origine, ce code ne devait servir à Microsoft que pour l'enregistrement de ses produits, Or ce même identificateur s'attache également aux fichiers créés par les applications Office. Plus grave, ce numéro peut être consulté via Internet par n'importe qui sachant comment y accéder. Une démonstration est d'ailleurs toujours en ligne sur le site de la société Pharlap qui "interroge" votre ordinateur et vous renvoie immédiatement vos numéros d'identification. Si cela vous rassure, cette fonction existe aussi dans Windows Me, XP, ...

Détruire les mouchards

Si vous souhaitez interdire la communication de ces numéros confidentiels à quiconque, il faut inhiber l'assistant d'enregistrement, ce qui, heureusement est assez facile : Cliquez sur le bouton Démarrer, puis Exécuter Dans la boite de dialogue, tapez : regsvr32.exe -u c:\Windows\system\regwizc.dll. Il ne vous reste plus qu'à cliquer sur OK. Le message "DllUnregisterServer in c:\Windows\system\regwizc.dll succeded" doit alors apparaitre.

Si ultérieurement vous souhaitiez rétablir cette fonction effectuez la même séquence, mais en tapant la commande inverse. regsvr32.exe -c c:\Windows\system\regwizc.dll. A noter qu'un fichier texte, appelé Reginfo.txt, peut également servir à vous identifier. Vérifiez s'il existe sur votre disque dur en lançant une recherche. Vous souhaitez le voir disparaître, simple, supprimez-le.

Nouvelle fonctionnalité

Microsoft a intégré récemment une nouvelle fonctionnalité dans ses logiciels qui permet, lors d'un bug, d'avertir et de créer un "rapport d'erreur". Seul hic, cette fonction semble cacher en son sein, un SpyWare. Comprenez par SpyWar, espiongiciel, un espion. Les applications qui sont appelés par Windows se nomment Dw.exe. D'après la notice OfficeXP DW.exe saisit les réglages de l'utilisateur reliés au "plantage" directement via la base de registres et du bloc de mémoire du logiciel fautif. DW rassemble ces informations, fichiers associés et utilisés par l'application "planteuses". Le Computer Incident Advisory Capability du département américain de l'Énergie, qui est à l'origine de la découverte de cet "espion", propose sur son site l'anti-spyware pour Xp et IE6.

En savoir Plus

Le site du Pharlap
www.pharlap.com
Anti mouchard pour Pentium III
ftp://download.intel.com/support/processors/pentiumiii/psfre103.exe
SpyBlocker
www.becky-users.morelerbe.com/spyblocker/
Ad-Aware
www.lavasoftusa.com/aaw.html
Web Sécurité spécialisé dans les SpyWar
www.websecurite.net

Mieux utiliser Google.com !

Le célèbre moteur de recherche Google est une vraie pipelette. Après avoir donné du grain à moudre aux pirates, en cherchant par exemple des logiciels de commerces en ligne buggués afin d'exploiter une faille. Aujourd'hui les options de Google permettent de trouver des mots de passe et des documents ultra sensibles.

Documents sensibles

A force de laisser traîner des informations sur des serveurs ultra protégés, les administrateurs négligents ne s'attendaient pas à ce que l'ami Google soit capable de garder en mémoire et d'archiver fichiers PDF (Abobe Acrobat), documents Word, Excel, PowerPoint. Là où le bas blesse est que n'importe qui peut se faire piéger, et pas que des sites militaires US. C'est le magazine canadien "Le Devoir" qui va lever le lièvre avec des sites militaires de l'Oncle Sam. Il faut savoir cependant que Google propose une option armée, avec une recherche uniquement dans des sites internet militaires US. Option nommée par Google, Uncle Sam.

Mots de passe, factures et compagnies

Le problème avec l'ami Google est que ce dernier réceptionne n'importe quel document. Il suffit de taper "document", "pdf", "doc", pour avoir le choix de sélectionner votre butin. Dans notre enquête nous n'avons pas eu besoin de taper dans les sites militaires pour tomber sur des informations confidentielles. Mots de passe de site internet, de compte e-mail, de gestion de service Wap, de quoi transformer certaines entreprises françaises en véritable capharnaüm à pirate.

Que faire ?

Deux possibilités s'offrent à vous. Ne rien faire ou alors enlever les documents sensibles de vos serveurs. D'ailleurs on se demande encore pourquoi des documents contenant des mots de passe, pour ne prendre que cet exemple, puissent se trouver sur le web. Il serait chiffrer encore ! La culture de la sécurité informatique a encore de bien beau jour devant elle.

En savoir Plus

Moteur «options» de Google
www.google.com/advanced_search?hl=fr

Phrack 57
www.phrack.org/show.php?p=57

SpyBlocker
www.becky-users.morelerbe.com/spy-blocker/

Google spécial Armée
www.google.com/unclesam

Pirate Intelligent

Imaginez une faille exploitée à distance et permettant de compromettre un système sans qu'aucune ligne de code ne soit directement envoyée à la victime. Imaginez un exploit qui créerait simplement un fichier en local afin de compromettre des milliers d'ordinateurs, et qui n'implique aucune source spécifique dans l'attaque. Voilà ce que peut faire aussi un moteur de recherche intelligent aujourd'hui.

Les exploits zéro-effort créent une 'wishlist', et la déposent quelque part dans le cyberespace - voire sur un serveur hébergé chez leur créateur, bref dans un endroit où d'autres peuvent les trouver. Ces "autres", ce sont les travailleurs invisibles de l'Internet. Ils sont des centaines à ne jamais dormir, infatigables chenilles parcourant sans fin la toile mondiale : agents intelligents, moteurs de recherche... Ils viennent pour sélectionner cette information, et - à leur insu - pour attaquer des victimes. Vous pouvez arrêter l'un d'eux, mais ne pouvez pas les arrêter tous. Vous pouvez découvrir ce que sont leurs commandes, mais vous ne pouvez pas deviner ce que ces commandes seront demain, cachés qu'ils sont dans l'abîme toujours inexploré du cyberespace.

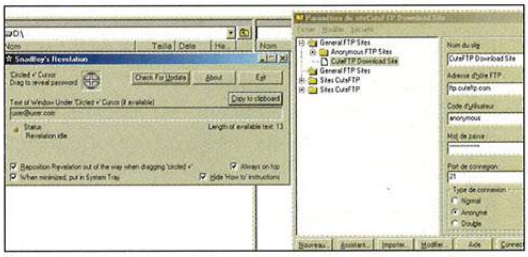
Bienvenue dans une nouvelle réalité, où nos machines, à l'intelligence plus que jamais artificielle, peuvent se lever contre nous. (Source : Extrait de Phrack #57, traduit et publié avec l'aimable autorisation de Michal Zalewski, que nous remercions.)

Appz!

Voici notre sélection de programmes à télécharger. Tous seconde : vous pouvez vous les procurer en vous rendant

Retrouvez vos mots de passe !

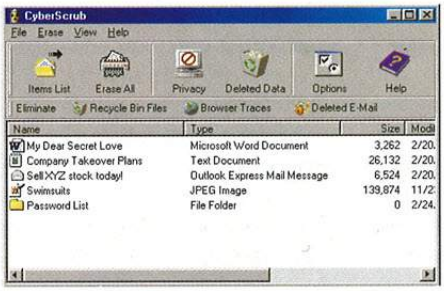
Nom : Révélation Langage : US Poids : 1,23 mo License : Freeware



Qui n'a jamais pesté devant les étoiles qui cachent nos mots de passe ? Je ne sais pas pour vous mais il y a des fois où j'oublie un mot de passe dont j'ai besoin par exemple pour un compte de courrier électronique ou encore pour accéder à mon serveur FTP. Le logiciel Révélation est parfait pour les têtes en l'air et son fonctionnement est des plus simples : vous lancez votre logiciel Révélation, vous lancez ensuite le programme étoilé. Vous sélectionnez le curseur cible et vous visez les étoiles. Par magie, ou presque, votre mot de passe va réapparaître dans une fenêtre dédiée.

Vivez heureux, vivez caché !

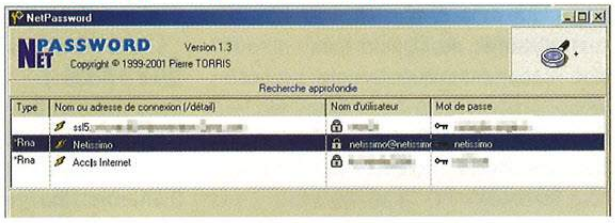
Nom : Cyberscrub // US | 0,90 mo | Shareware



Le programme Cyberscrub retire toutes les traces que vous avez pu laisser en utilisant un micro-ordinateur. Des fichiers temporaires Internet, aux cookies, en passant par la mémoire cache, tout est effacé rapidement et efficacement. Il sera dès lors impossible à un tiers de détecter un quelconque signe d'activité sur le micro traité avec ce programme.

Pour ne plus jamais perdre ses mots de passe d'accès Internet

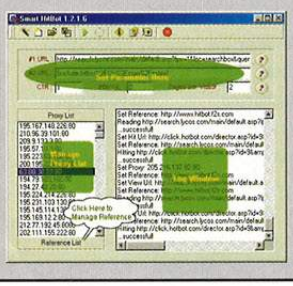
Nom : NetPassword // FR | 0,50 mo | Freeware



Listez toutes les connexions disponibles de votre système en affichant pour chacune d'elles : le nom de la connexion, le nom de l'utilisateur (identifiant), et le mot de passe relatif, ce dernier étant directement décodé et affiché en clair ! Cette version dispose également d'une recherche approfondie susceptible de lister les mots de passe de certaines pages Web. Les options du menu contextuel permettent d'afficher les propriétés d'une connexion, de lancer directement une connexion, ou encore de copier toute la liste dans le Presse-Papiers.

Ce programme clique les bannières pour vous !

Nom : Smart Hitbot Langage : US Poids : 0,80 mo License : Shareware

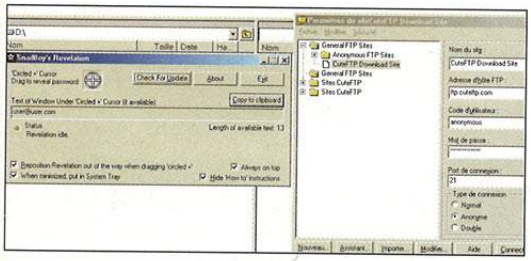


Ce programme, assez original, permet d'automatiser le clique ou la visualisation de bannières. En configurant votre programme, vous lui spécifiez quelle bannière cliquer, combien de fois, avec combien de temps d'intervalle s'il lui faut lire plusieurs bannières avant d'en cliquer une, et voilà le programme parti tout seul cliquer des pubs pour vous ! A noter qu'il est même possible de lui faire changer de proxy, ce afin d'utiliser à chaque fois une adresse ip différente. Ce programme est un shareware, essayable pendans 15 jours !

vont rendront de grands services alors n'hésitez pas une sur http://mag.zataz.com !

Mots de passe de fichiers Zip

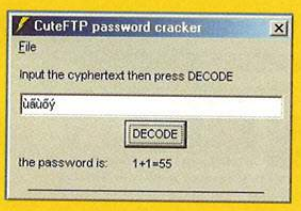
Nom : Advanced ZIP Password Recovery Langage : FR Poids : 0,49 mo License : Freeware



Ce logiciel est d'un autre genre, il utilise une manière et une technique de travail beaucoup plus lourde que les logiciels testés. Créé par deux informaticiens russes, Vladimir Katalov et Andy Malyshev d'Elcom LTD. Ce logiciel utilise la technique du brute force pour retrouver un mot de passe utilisé dans un fichier compressé par le format ZIP. Le principe est simple, vous sélectionner ce que vous souhaitez déchiffrer et il ne reste plus qu'à prier. Le déchiffrage peut durer quelques minutes à quelques siècles. Un temps de recherche qui va varier selon la taille, la diversité et le nombre de signes utilisaient par ce mot de passe.

Bloqué sur Cute FTP

Nom : CuteFtp Hack // US | 0,90 mo | Shareware



Il existe une petite application simple comme bonjour qui va pouvoir vous aider à retrouver votre mot de passe utilisé par CutFTP, pour accéder à la gestion de votre site web. Le logiciel se nomme CuteHack. Il est simple d'utilisation, il vous suffit de trouver le fichier SW de votre logiciel et a déchiffrer votre password oublié.

Sécurisez votre Mac !

Nom : Macintosh hacker's workshop // Fr | 0,96 mo | Freeware

Code511, société d'audit informatique propose, pas le biais d'un de ses membres, "Grungie", un outil de sécurité pour Mac, en Open Source. L'outil se nomme Macintosh Hacker's Workshop, il va vous permettre de vous sécuriser de maniére efficace. Enfin un outil pour MAC, il serait dommage de le laisser passer.

Téléchargez la barre de Zataz Magazine !

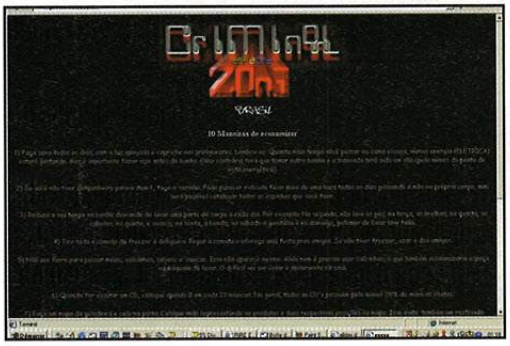
Nom : ZATAZ Barre sécurité Langage : Fr Poids : 0,50 mo License : Freeware

On termine cette sélection par l'un de nos logiciels nommé la ZATAZ Barre Sécurité. La ZATAZ Barre va vous permettre de surfer et d'utiliser votre machine avec les premières sécurités de base pour son PC. Vous allez pouvoir, par exemple, empêcher toute modification de votre bureau, navigateur, connexion, afin de bloquer toute tentative de piratage. Vous allez aussi pouvoir contrer un trojan, scanner les ports de votre machine pour apprécier la visite ou non d'un intru, un firewall ainsi qu'une cinquantaine d'autres options de sécurité et des options utiles.

Hacked!

Les sites piratés du mois !

Il s'en passe de drôles sur la toile. Voici notre sélection de sites internet piratés soit par des script-kiddies en mal de reconnaissance ou bien par des hacktivistes. Une chose est sûre, l'imagination n'est pas toujours au rendez-vous. Ecrivez nous pour nous signaler des sites piratés !



Cible : www.9telecom.fr

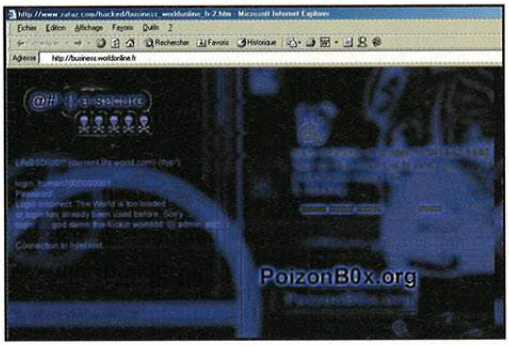
Auteur : Criminal Zone

Notre opinion : Criminal Zone est un hacktiviste brésilien anti-mondialisation. Dès lors, on comprend mal pourquoi il s'en prend à 9 Telecom...à moins qu'il se soit fait tuyauté une faille par des français.....:-)

Cible : www.benetton.de

Auteur : Brazil Hackers Sabotage

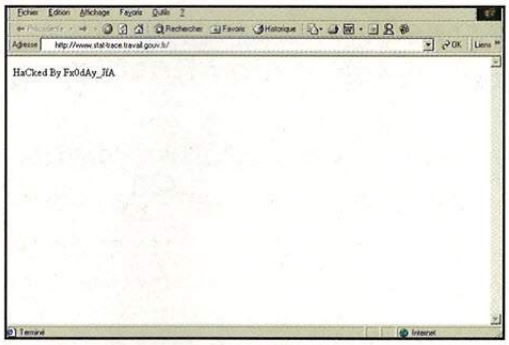
Notre opinion : Avec l'hiver, même les pirates veulent se couvrir. Benetton, le roi du pull en a fait les frais. C'est la première fois qu'un site Benetton se fait retourner la pelotte !



Cible : business.worldonline.fr

Auteur : Poizon Box

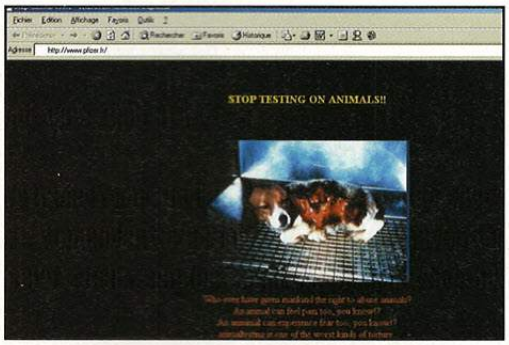
Notre opinion : L'un des groupes les plus actifs de la planète Pirate se paie le serveur entreprise du fournisseur d'accès français World on Line. Ce n'était pas la première visite, mais déjà la deuxième !



Cible : www.stat-trace.travail.gouv.fr

Auteur : FxOday

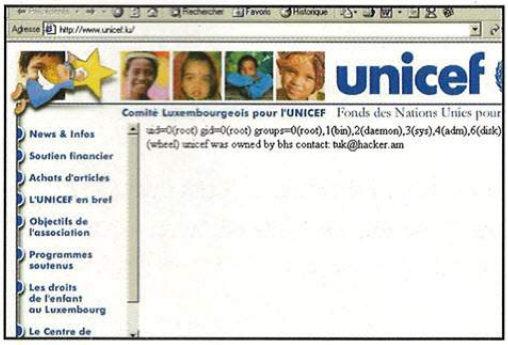
Notre opinion : Suffisamment rare pour le remarquer, un site du gouvernement français piraté sans grande raison. On présume que le ministre a dû apprécier !



Cible : www.pfizer.fr

Auteur : Theli et Mitsai

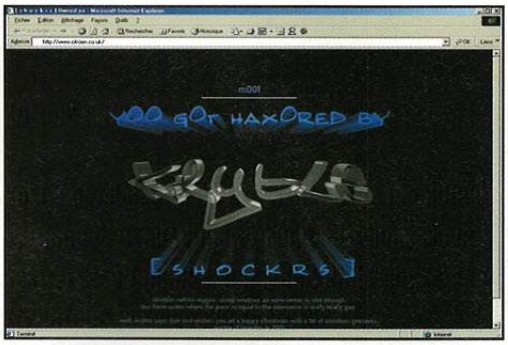
Notre opinion : De l'Hactivisme pur et dur pour deux hackers qui demandent à ce laboratoire pharmaceutique de stopper leurs essais sur les animaux. Images choc pour sujet difficile...



Cible : www.unicef.lu

Auteur : Tuk

Notre opinion : Le site luxembourgeois de l'UNICEF, organisation connue pour tenter d'aider les enfants dans le monde, a connu les joies d'un script kiddie qui aurait mieux fait d'apporter son soutien plutôt que sa bêtise !



Cible : www.citroen.co.uk

Auteur : Kryble

Notre opinion : Ce pirate a du rater plusieurs fois son permi de conduire au volant d'une Citroën. Nous ne voyons que cette raison pour s'acharner de la sorte sur le site du constructeur automobile français.

Courrier

Cette page est à vous. Posez-nous vos questions, vos idées, vos remarques. On répondra dans la mesure du possible sur cette page. On répondra à tous par e-mail. Pour nous écrire contact@zataz.com

Spam attaque

Bonjour,
Je viens de recevoir une publicité non sollicité dans ma messagerie électronique. Que faire pour empêcher cela ?
Daniel Plaisant , Rouen

Le moins que l'on puisse dire est que les spams, les publicités non sollicitées, continuent de remplir nos boites à e-mails. Que faire face à ce genre de courrier ? Soit vous vous êtes inscrits et vous avez oublié ou alors un petit plaisantin vous a enregistré. Il vous suffit alors de renvoyer un e-mail vide avec dans la partie "Sujet" de votre courrier le mot "Remove" ou "désinscription". Dans la mesure ou aucune adresse d'émission n'apparaît, allez dans la partie "Message" de votre Outlook et sélectionnez "Bloquez expéditeur".

Stopper les pédophiles

Bonjour,
Je suis choqué par ce que je viens de voir. En surfant je suis tombé sur un site pédophile proposant des milliers de photos d'enfants. Il n'y a pas moyen de les pirater ?
Maxime Kouyoumdjian

La pédophilie sur Internet ne se combat pas à coup de "piratage". Le mieux est encore d'en informer les personnes qui sont en charge de lutter contre ce fléau. Si vous avez repéré un site de cet acabit. Notez son URL et soit vous vous dirigez vers une association d'aides à l'enfance, comme l'association du Bouclier - Bouclier.org - soit vous en informez la Police, la gendarmerie qui ont des équipes spécialisées dans ce genre de traque.

Droit de copie

Salut ! Je voudrais copier le logiciel que je viens d'acheter, est-ce que j'ai le droit ?
Stéphanie Vacher

Si vous êtes détenteur de l'original, que vous avez l'intention de faire une copie de sauvegarde, que vous ne souhaitez pas le mettre à disposition par un quelconque moyen, oui, vous pouvez faire une copie de ce logiciel.

Emulateurs et jeux consoles

Bonjour,
Je voudrais mettre en ligne un site sur les émulateurs de consoles de jeux. J'ai entendu dire qu'il était possible de mettre des jeux en ligne à la condition d'y mettre aussi un avertissement.
EmulBoy

L'avertissement, le Disclamer, annonçant que vous pouvez télécharger un jeu console et le garder 24 heures est totalement faux. La ROM game boy, SNES, N64, ... est considéré comme une copie, donc une contrefaçon. La mise en ligne est possible dans la mesure ou le jeu a été mis en libre de droit par les éditeurs. On vous invite à lire le magazine les Puces informatiques qui reviennent souvent sur le sujet de l'émulation.

Gens d'armes numériques

Bonjour,
Je voudrais mettre en ligne un site sur les émulateurs de consoles de jeux. J'ai entendu dire qu'il était possible de mettre des jeux en ligne à la condition d'y mettre aussi un avertissement.
EmulBoy

Il est tout à fait possible de tracer quelqu'un à partir d'un site web. Pour cela il suffit de mettre en place certains outils sous forme de CGI ou autres. Ces petits programmes pourront permettre d'intercepter IP, zone de connection, ... Il faut savoir que si le site en question agit ainsi, les outils d'analyses de connections permettent aussi de savoir qui vient faire quoi sur un site web. Pour ce qui est du site cité, je doute qu'ils agissent ainsi.

Vous êtes passionné par l'underground, le piratage et le hacking ?
Vous souhaitez faire partager
vos connaissances ou vos scoops dans Zataz Magazine ?
Si oui, écrivez nous pour tenter de rejoindre notre équipe !

Découvrez vite le 1er Magazine Internet de poche !

Le 1er magazine internet de poche !

Net@scope

N° 47 - Décembre 2001

Révolutionnaire :

Internet par ondes radio

le haut débit pour tous et partout !

Webmasters

Vendez votre contenu par téléphone !

Shopping de Noël :

Les bonnes affaires
Les sites à franchement éviter

Les 20 logiciels de l'année à télécharger !

+ des scripts et des astuces pour votre site !

15 FF chez votre marchand de journaux

mag.zataz.com