PIRATAGE - HACKING - VIRUS- CARDING - PHREAKING - WAREZ

ZATAZ

ZATAZ

HACKERS & PIRATES MAGAZINE

N° 7

Bimestriel - Belgique : 2,3 Euros - Suisse : 4 CHF

M 05129 - 7 - F: 2,00 € - RD

USIF EXLUSIF EXCLUSIF EXCLUSIF EXCLUS

special ARNAQUE

Tricher aux casinos internet
Les gadgets high-tech pour gruger aux examens

Et on parle de ça aussi :

Utilisez Linux sans l'installer !
Les pirates s'attaquent au porno
Palladium, l'arme fatale de Microsoft
La scène Warez française en photos !

SIF EXLUSIF EXCLUSIF EXCLUSIF EXCLUS

SPECIAL

Prolongations !

Le hors-série et son CD-ROM restent en vente jusqu'à la fin du mois ! Dépêchez-vous de vous procurer un exemplaire avant la rupture de stock !

Le 1er hors-série de Zataz Magazine est en kiosque.

Copiez vos jeux vidéo, dézonez vos lecteurs DVD, découvrez les secrets du DivX...

SOMMAIRE

Nous sommes un magazine dédié à la sécurité informatique, aux hackers, pirates, virus et warez. Un magazine différent de ce qui existe déjà car nous ne souhaitons pas vous transformer en cyber-délinquants, en hackers, en super- pirates. Notre but est plutôt de vous faire comprendre comment devenir un citoyen du web. Un internaute qui a des droits et des devoirs. Pas question pour nous de faire dans le binaire. Le j'aime/ j'aime pas est trop réducteur.

Aujourd'hui l'informatique est devenue un outil qui peut se retourner contre nous, les utilisateurs. Plus question de penser que l'Internet de 2003 ressemble à celui des années 90. Le filtrage, la surveillance, la manipulation, le piratage de nos vies... Le livre Orwell, 1984, avait commencé à nous parler de notre avenir. Il n'avait pas tout prévu. Aujourd'hui les curieux du web, les hackers, sont criminalisés au même titre qu'un cyber-escroc, un e-voleur... Le hacker n'a rien d'un génie, d'un magicien... ni d'un monstre. Son but ? Faire avancer ses connaissances, celles des autres en alertant la communauté, celle qui utilise l'informatique, des problèmes de sécurité ou d'intrusion dans nos vies privées. C'est pour cela que dans ce septième numéro de ZATAZ Magazine, nous avons voulu vous montrer que l'informatique et l'internet sont des filles sexy qu'il faut savoir ménager.

Dans ce septième "ciel" numéro, nous avons voulu vous montrer que l'Internet peut être un piège pour celui qui n'y prend pas garde. L'armée US annonce des sites ultra protégés, on vous montre le contraire. Vous aimer jouer au casino, découvrez comment certains pirates trichent. Heureusement, le web c'est aussi, et avant tout, des contacts, l'envie de connaître, de comprendre l'autre, comme le service de renseignements internet de la police Suisse qui préfère parler aux hackers pour mieux attraper les pirates.

Nous ne sommes pas peu fier de vous présenter ce nouveau numéro de ZATAZ Magazine. En espérant que vous prendre autant de plaisir à le lire, que nous à le faire.
Bonne lecture, on se retrouve début juillet.
Damien Bancal

Abonnes-toi page 29
et rejoins la communauté ZATAZ !

Zataz Magazine : 61, rue Jouffroy d'Abbans, 75 017 Paris. Fax: 01.40.53.86.44 E-mail : mag@zataz.com, web : www.zataz.com
Chef de la rédaction : Damien Bancal
Ont collaboré à ce numéro : Eric Romang (Lux), Christophe Schleypen (Be), Benoît Guignard (Uk), Benoît Beaulieu, Stéphie Reinruof, Antoine Santo.
Correspondants : Nita et Ngyuen (Hong-Kong), Nihiatu (Dheli, Inde), Guillaume, Sam et Lucile (USA), Jeff et David - Correspondant (Tel-Aviv, Israël)
Conception graphique : Tomahawk Studio (thx Patrice !) Impression : Léonce Deprez, Béthune Distribution France : NMPP - Belgique : AMP
Commission paritaire : 0707 T 81854 Dépôt légal à parution
Service des ventes : Distrimédias, tél. : 05.61.72.76.72 - fax : 05.61.43.49.50
Directeur de la Publication : Charles Daleau
Editeur : Mediastone, 61 rue Jouffroy d'Abbans 75 017 Paris . Siret : 422990015200019 - Code APE : 221E

Reproduction partielle ou totale interdite sans l'autorisation écrite de l'éditeur. Les documents envoyés à la rédaction ne sont pas rendus à leur expéditeurs.

Quand la musique est bonne ...

Les maisons de disques viennent maintenant prévenir les médias que les prochains albums de leurs chanteurs se trouvent déjà en version pirate sur Internet. Emi Musique vient aussi d'avouer de son côté utiliser de faux MP3 de Radiohead afin d'envahir les réseaux peer-to-peer de fausses copies et ainsi freiner les téléchargements intensifs. Ces contrefaçons volontairement ratées contiennent du souffle ou ne sont pas complètes. Gageons que ces manœuvres ne risquent pas d'empêcher les fanas de MP3 de sévir !

Piratage de masse

Un Déni de Service Distribué, un DDoS, a vidé les serveurs de l'ISP Américano-hollandais, DOT Tk. Cette attaque lancée à partir d'une dizaine d'ordinateurs a perturbé plus de 400.000 sites, dont 80.000 aux Pays-bas. Elle a également bloqué les routeurs de cette société basée à Amsterdam et à San Francisco, spécialisée dans la vente de nom de domaine en .tk, suffixe tiré du nom de l'île de l'Océan Pacifique Tokélao. Si le ou les pirates de cette affaire ne sont pas connus, il est intéressant de remarquer que les attaques à l'encontre de sociétés utilisant le nom ou la culture des habitants de certaines îles du pacifique sont de plus en plus courantes. Pour ce qui est des attaques de DDoS, elles aussi sont devenues fréquentes depuis plusieurs mois.

2 millions de dollars

Les militaires américains louchent sur le travail du hacker, l'inventeur d'OpenBSD, Theo de Raadt. Ce dernier vient ainsi de recevoir 2 millions de dollars du DARPA, le Defense Advanced Research Projects Agency. Intéressant de voir que le DARPA se moque de la version Linux de la NSA.

La bourse ou la vie

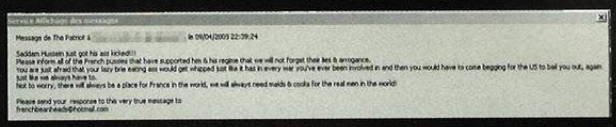
La bourse de Séoul a chuté temporairement fin mars après que des chaînes de télévision sud-coréennes, MBC TV, YTN et SBS TV, ont annoncé l'assassinat de Bill Gates. L'indice de référence a perdu 1,5% à la suite de ce hoax. La rumeur était partie d'un faux site CNN. (Source : AFP)

5312

Nouvelle découverte ZATAZ Magazine avec l'hébergeur franco-suisse net-advanced.com. Ce dernier souffrait d'une faille malheureusement commune qui ouvrait la page administration de cette société offrant du même coup la possibilité de créer des comptes, de modifier les infos clients, DNS... Prévenu dans la seconde de notre découverte, la correction a été faite après notre coup de téléphone. Nous signons ici notre 5.312e coup de main à une société française sur Internet.

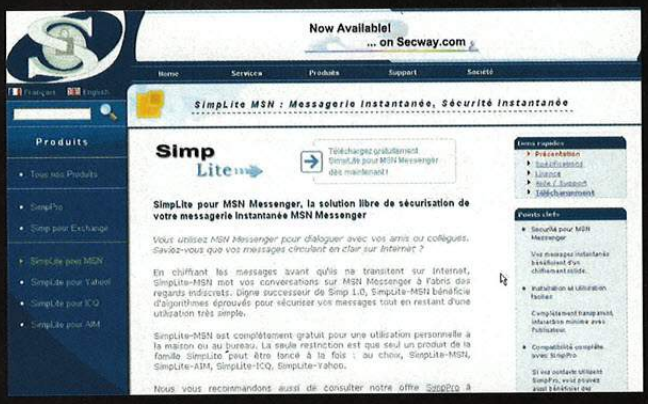
BUSH DANS VOTRE PC

Plusieurs lecteurs nous ont fait part de l'apparition de fenêtres intrusives lors de leurs connexions à MSN messager. Sitôt le programme lancé, ces fenêtres pop-up apparaissent, affichant un contenu est loin d'être sympathique puisqu'il s'agit d'une série d'insultes provenant sans doutes d'américains, à l'encontre des pauvres français que nous sommes. Détail intéressant techniquement, ces pop-up ne s'ouvrent que si le fournisseur d'accès de la « cible » a une extension en « .fr ».



BON PLAN

La société française Secway vient de sortir sa nouvelle monture de SIMP, traduisez par Secway's Instant Messenger Privacy. SIMP va chiffrer vos messages de manière efficace et facile sous MSN, Yahoo, ICQ et AOL. Une clé de chiffrement va être crée et diffusée à vos correspondants et vous permettra de chiffrer à la volée vos informations sans crainte de lecture par une tierce personne.



VOUS AVEZ UN MESSAGE

Un pirate informatique a fait irruption début avril dans le compte du courrier électronique d'un membre du Congrès américain, Ginny Brown-Waite. Chose étonnante, cette députée avait fait parler d'elle le mois dernier en proposant une loi qui imposait le rapatriement des soldats américains enterrés en France lors de la seconde guerre mondiale. Le FBI tente de retrouver le pirate qui a diffusé, via l'e-mail de la députée, des messages contre la guerre en irak et proposé que la peine de mort soit appliquée à George W. Bush, au Vice-président Dick Cheney et au Ministre de la Défense Donald H. Rumsfeld. Pour information, menacer de mort un élu américain est passible de la peine maximale.

COUP DE POUCE

Les surfs sur le réseau sont pleins de surprises. Autre découverte de ZATAZ Magazine, deux services de créations de sites marchands : oxygene.ws de Memsoft Mutlilog et citybizz.net. Ces deux sites souffraient d'un problème de taille, un accès à la page d'administration via un module non protégé par une faille SQL. Prévenu dans la seconde de notre découverte, il faudra attendre 8 jours et un appel téléphonique de notre part pour que ces deux sites réparent le problème. L'important est que ces deux hébergeurs soient dorénavant protégés.

CAGE NUMÉRIQUE

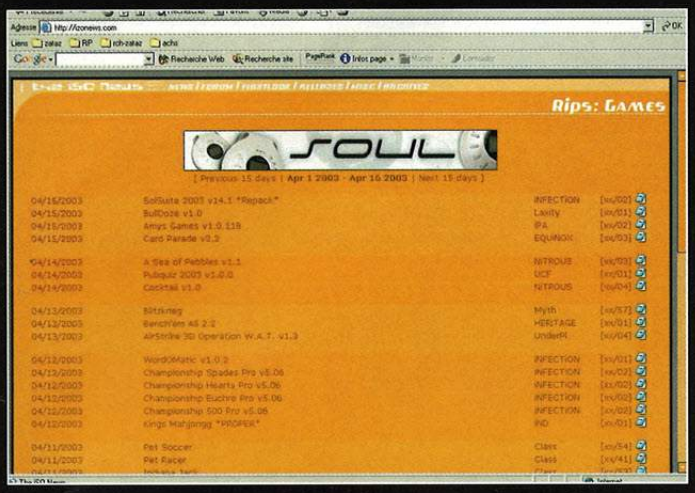
Le brevet a été enregistré sous le numéro WO 03/005666. Le journal New Scientist explique que derrière ce code se cache une solution mise au point par Intel pour arrêter des attaques Internet de type"Déni de Service Distribué"
(DdoS. Un DoS, "Déni de Service" correspond à une attaque visant à bloquer un ordinateur en lui envoyant un nombre important d'information. Un DDoS est la même technique mais via plusieurs machines assaillantes.

MASSE ATTAQUE

Nouvelle attaque à l'encontre du serveur Irc Undernet. Cette fois-ci, plusieurs centaines de bots, des petits robots agissant sur IRC, sont venus envahir ce serveur début avril. Ils ont exploité la faille IPC en null session via des machines transformées en Zombies, afin de lancer cette attaque qui semble avoir eu pour but de saturer Undernet.
La faille IPC est un problème de sécurité cher aux groupes warez qui permet de diffuser des productions contrefaites sur des machines piratées.

DANS LES BAS FONDS MARINS

ZATAZ Magazine découvre un étrange pavillon sur le site www.riantec.com, page web de la commune du même nom, géographiquement située dans le Morbihan.
En empêchant le plugin Flash de fonctionner, un étrange message apparaît. Texte que l'on retrouve dans le code source de ce même site : « Our tanks to the fabulous Hackers DIabOlaX and Mr-I for helping us to secure our servers. » Le pirate en question, DIabOlaX, fait partie d'un groupe de pirates nommé Game0v3r Crew. Situation géographique probable, le Brésil. Fait étrange, alors que sur le site breton le pirate signe la correction du serveur, on peut voir un défacement beaucoup plus visible sur le site aquastream.fr. (Merci à Guillaume)



ISO NEWS

Le site Isonews était connu pour être une sorte de bibliothèque d'informations liées aux contrefaçons sorties dans le milieu warez. Son webmaster, David Rocci, n'avait rien à se reprocher à donner ce genre d'actu. Seulement l'appât du gain ayant été le plus fort et il a voulu gagner quelques dollars en commercialisant des puces pour consoles de jeux. Il n'y a pas été de main morte en important pas moins de 450 puces pour XBox. Il vient d'être condamné à 10 mois de prison, dont 5 fermes avec un bracelet électronique qu'il devra porter chez ses parents et à 28.500 dollars d'amende. Il risquait 5 ans de prison et 500.000 dollars d'amende. On va dire qu'il s'en sort plutôt bien. Le site est réapparu sous l'adresse izonews.com

LE MILLION, LE MILLION, ...

Voilà qui va amuser les amateurs du jeu "Qui veut gagner des millions". La justice britannique vient de juger trois arnaqueurs qui ont tenté de piéger l'émission "Who Wants to be a millionnaire ?" britannique. Comment ? Alors que le joueur écoutait les questions, une personne dans le public, un complice, toussait deux fois pour donner la bonne réponse. Les preneurs de son qui ont passé l'émission à régler le problème sonore lié à ce "malade" se sont rendus compte de l'anarque. Les joueurs viennent d'être condamné à 12.000 et 28.000 euros d'amende. Les tentatives de piratages dans les jeux T.V. ne sont pas une nouveauté. TF1 a vécu un piratage en 1998 lors de l'émission "L'or à l'appel". Des employés de France Télécom avaient piégé la ligne téléphonique de l'émission s'assurant ainsi le privilège d'arriver toujours en tête de liste pour être pris à l'antenne et gagner de l'argent.

LA PILULE PASSE MAL

Des milliers de patients pourraient avoir reçu de mauvais médicaments délivrés sur ordonnance.
Comment est-ce possible ?
Une coupure de courant a touché le centre informatique de Kaiser, basé en Californie du Sud. L'informatique tombée en rade permettait l'étiquetage de la pharmacie de l'hôpital. Environ 4.700 patients ont été affectés.

BUG BANCAIRE

Voilà qui laisse perplexe.
Imaginez que vous êtes un étudiant de l'université Princeton et que vous ayez décidé de sauter le pas : acheter des livres via la boutique online de la fac. Vous rentrez les identifiants qui vous ont été donnés et vous voilà face à 15 comptes bancaires qui additionnent à eux tous plus de 9 millions de dollars.
Voilà l'histoire qui vient d'arriver à Ira, gentil étudiant qui goûtait pour la première fois aux joies de l'achat en ligne. Pourquoi un tel bug ? L'identifiant d'achat du magazine recherché par l'étudiant était le même que l'identifiant bancaire de l'école. Un hasard à 9.9 millions de dollars, qui dit mieux !

LE VER DANS LA POMME

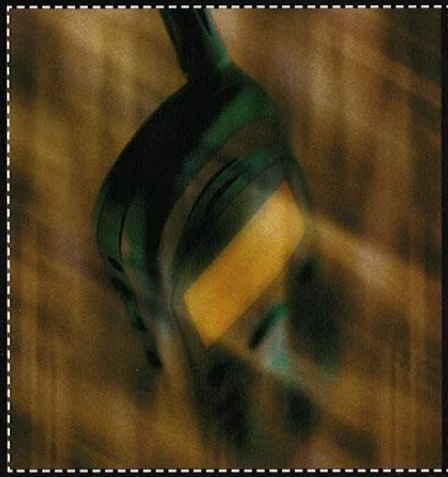
La société Janteknology vient de découvrir à ses dépends que l'ennemi ne vient pas obligatoirement de l'extérieur. Cette entreprise spécialisée dans la sécurité informatique a dû fermer ses portes et arrêter ses activités après le piratage d'un employé "fâché". Voilà qui est fâcheux !

LE WEB, UNE GRANDE ÉQUIPE

Comme tout bon sportif qui se respecte, le journal l'Equipe fait partie des bibles de ZATAZ Magazine. Le site aussi, avec une attention plus soutenue il y a quelques jours, après la découverte d'un lien plus qu'étrange dans l'une des pages. Ce lien renvoyait sur les IP de connexions FTP, administration ainsi que sur le login et le mot de passe, en clair, pour la mise à jour du site. Bref, des informations qui entre de mauvaises mains auraient pu permettre à un pirate de faire des bêtises ! Prévenu, le problème a été corrigé.

ATTAQUE DE MASSE

Le fournisseur Tiscali a vu ses serveurs chauffer au Royaume-Uni. Un ou plusieurs pirates ont lancé une attaque ayant pour but de bloquer les serveurs de ce FAI, attaque de type DDoS, Déni Distribué de Service, ayant visé le portail, les accès au web et les services mels de Tiscali. Cela commence à être de la routine pour Tiscali Uk qui a vécu sa seconde attaque de ce genre.



BOUILLEUR DE GSM

Un britannique a été accusé d'avoir utilisé et commercialisé des brouilleurs de téléphones portables. Glenn Jeffery Darien, 40 ans, a plaidé coupable. C'est l'agence des Radiocommunications qui a lancé l'enquête et qui est tombée sur la boutique de Darien. On pouvait y acheter un boîtier brouillant les communications GSM mais qui permettait de perturber aussi les communications de la police, d'ambulances ou des feux rouges.
Dans ce dernier cas, rien n'empêche de penser qu'il aurait été capable de faire passer au vert les feux tricolores de son choix.
L'utilisation d'un brouilleur est une infraction qui est reconnue par la loi depuis 1949 par le "Wireless Telegraphy Act".
A noter qu'en France ce genre de « gadget » est également illégal.

Main dans la main, main dans la tronche !

Le site web d'Al-Jazeera, le CNN du Moyen-Orient, vient de se voir refuser l'aide d'Akamai, hébergeur et célèbre diffuseur de contenu par liaisons très haut débit.
Al-Jazeera souhaitait pouvoir contrer les pirates, mais aussi, faire face à une sérieuse montée en charge de ses serveurs suite à la guerre en Irak.
Parmi les 12.600 clients d'Akamai, citons le F.B.I ou encore C.N.N. Pour rappel, le créateur d'Akamai est mort dans l'un des avions du 11 septembre.

Number 6

Jason Jarrell, un jeune internaute américain aujourd'hui âgé de 19 ans et pirate à ses heures perdues risque 95 ans de prison.
Son crime est d'avoir pénétré les serveurs de l'université de Yale en 2000 et de s'être intéressé de trop près au laboratoire de résonance magnétique nucléaire de cette université.
Résultat, des dégâts évalués à 150.000 dollars ! Le gamin avait été retrouvé grâce à son fournisseur d'accès.

E-vote vérolé

Voilà qui va amuser les détracteurs du vote électronique. Un virus a perturbé le vote électronique mis en place dans la commune de Will County, Illinois.

Les électeurs n'ont pu envoyer leurs e-bulletins en raison du blocage, par un virus, du serveur qui centralisait les votes. Ce virus qui a perturbé l'élection du Maire serait parti du Japon.

Super base de données

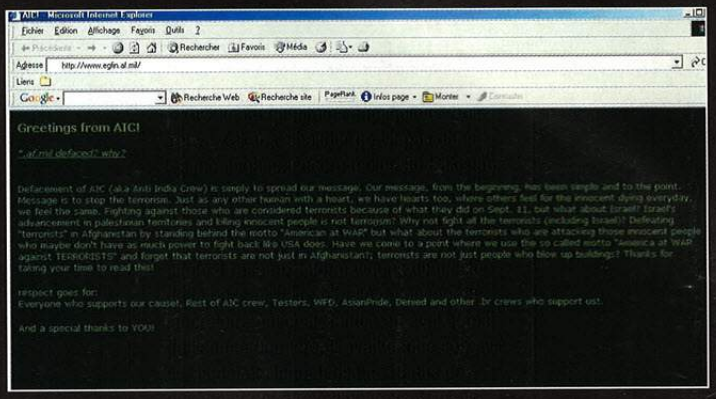
Les fonctionnaires du FBI ont annoncé qu'ils examinaient actuellement une version limitée d'un système électronique pour contrer terroristes et autres cyber-pirates. Terroristes, cartels de la drogue et pédophiles sont dans le giron du FBI qui va constituer une super base de données des criminels du monde entier.

Couac dans le portable

Le Washington Post explique que plusieurs cas d'erreurs d'aiguillage ont failli coûter la vie à des personnes en danger, utilisant leurs téléphones portables pour appeler les forces de police via le 911.

Il s'avère que selon le quartier d'où étaient lancés ces appels d'urgence, les antennes redirigeaient la communication vers les mauvais commissariats.

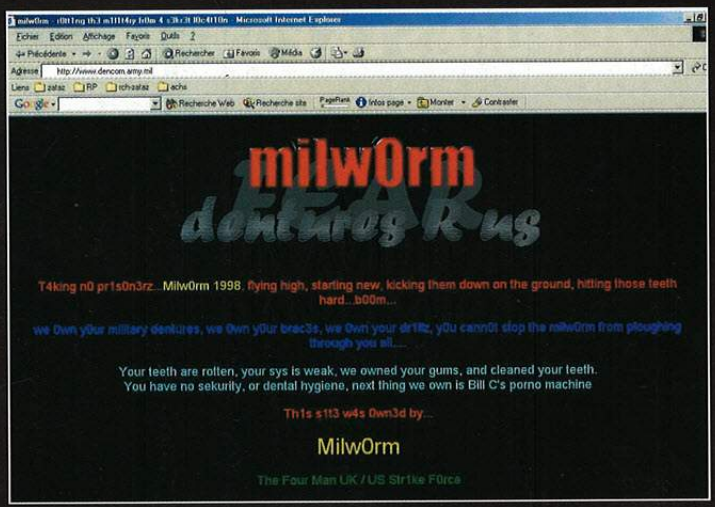
USURPATEUR



Il avait signé sous le pseudo du groupe AIC, team de pirates anti-indiens. Adil Yahya Zakaria Shakour ne vit pas dans les montagnes, encore moins au Pakistan. Du haut de ses 18 ans, il vivait tranquille à Los Angeles avant que le FBI vienne lui taper sur l'épaule. Il a été accusé d'avoir piraté 4 réseaux informatiques dont celui de la base militaire d'Eglin ou encore du laboratoire national Sandia en avril et mai de l'année dernière. Il avait donné son avis sur Israel et l'Inde. Il risque 15 ans de prison pour quatre malheureuses "pages index" modifiées. Autant réfléchir à dix fois avant de vouloir jouer au defaceur ! Le Sandia National Laboratories est une cible plutôt courante chez les pirates, à se demander même si le serveur de ce dernier n'est pas un Honey Pot, un pot de miel à defaceurs. Plusieurs cyber-délinquants sont déjà passés par-là, comme Prime suspectz.

PAS DE NEZ ROUGE POUR LES CLOWNS

Le site parodique sur la Maison Blanche, Whitehouse.org, menacé par des avocats. Le webmaster a voulu donner son avis sur la politique de son pays, les USA, en plaçant un nez rouge sur le nez de la femme du vice-président Dick Cheney. Mauvais plan, le Dick a menacé le webmaster, John Wooden, d'un procès.



CENTRALE NUCLÉAIRE

Il avait signé VeNoMouS, du groupe Milw0rm. Jodi Jones a plaidé coupable devant un tribunal de Manukau, Nouvelle Zélande, pour le piratage de sites internet entre 1998 et 2000. Parmi ses cibles, une centrale nucléaire indienne, celle de Bhabha. Agé de 23 ans, il a nié être l'auteur de ces piratages, mais l'enquête semble prouver le contraire. Il avait utilisé une faille dans le programme SSH en y insérant une backdoor nommée Frozen. A l'époque VeNoMouS avait expliqué qu'il avait été formé par Ehud Tenebaum, un adolescent israélien connu sous le pseudo Analyzer. Le juge a proposé 100 heures de travail d'intérêt général.

TEE-SHIRT

Vetour du soleil et de la chaleur. Vous allez être beau dans les tee-shirts ZATAZ Magazine ! Nous proposons une dizaine de modèles pour homme, femme et enfant. http://www.zataz.com

J'AI LA MIGRAINE

Voilà qui ne va pas les aider à dormir ! Environ 7.000 patients du Centre de l'Université de l'Indiana se sont fait pirater leurs dossiers médicaux.
Des personnes ayant des troubles du sommeil. Numéros de Sécurité Social et autres informations personnelles ont pu être volées. Personne ne sait vraiment si les dossiers ont été téléchargés, les administrateurs savent seulement qu'un pirate est passé par-là le 27 novembre dernier. Cinq mois pour s'en rendre compte, ils dormaient ou quoi ?

COMME UN AVION DANS L'AIR !

La vente aux enchères sur eBay d'un manuel de vol dérobé dans un aéroport a incité la police à mettre la main sur un bagagiste d'Air Canada. Robert Gaglione, 47 ans, a volé une édition du manuel de vol que seul les pilotes peuvent posséder et l'a mis en vente sur le site eBay. Le document contenait des informations liées à la sécurité, comme les sièges attribués aux policiers en civil, chargé de la protection de l'avion, ou encore, quel personnel de vol possède la clé de la porte de la cabine des pilotes.

LES SECRETS DES CASINOS EN LIGNE

M. X est administrateur dans un important casino en ligne. Qui mieux que lui pouvait nous parler de son métier où secret et discrétion sont de mise ? En exclusivité pour ZATAZ Magazine, ses employeurs lui ont donné l'autorisation de répondre à quelques-unes de nos questions.

Les casinos Internet sont devenus des cibles privilégiées pour certains pirates, pouvez-vous confirmer ?

Difficile à l'heure actuelle d'évaluer le phénomène, car nous n'avons eu que connaissance d'attaques chez d'autres opérateurs.

Vous gérez un casino, je suppose que pour vous la sécurité est une obligation. Comment est-elle mise en place ?

Un casino en ligne se sécurise de la même façon que n'importe quel autre site : Firewall, détection d'intrusion, mises à jours... mais aussi comme tout centre de calcul vraiment sécurisé (accès très restreints et surveillés tant par les mots de passe que physiquement aux machines). Les mesures complémentaires utilisées sont du type détection d'activité "anormale" (vitesse de jeu trop élevée pour être le fait d'un humain, gains "hors normes", etc.) qui peuvent déclencher des alarmes ou des suspensions de service pour un utilisateur ou globales.

Avez-vous connu des cas de tricherie pour un casino Online ?

Non, pas encore. Cependant nous avons eu connaissance de tels faits chez des casinos déjà en ligne.

Et pour un casino "physique", un vrai casino ?

Oui ! Caméras miniaturisées, transmetteurs radio, calculatrices... Il semble que la seule limite soit la motivation du tricheur, car l'imagination est sans borne.

Nous avons découvert des dizaines de casinos faillibles à des failles "idiotes". Nous aurions pu changer les informations des sites, les % de reversement des jackpots, les programmes à télécharger... Comment reconnaître un casino Internet digne de ce nom ?

Tout d'abord, dans la plupart des cas, les jeux ne se font pas sur le serveur web. Donc une modification de celui-ci serait sans conséquence sur le jeu lui-même. De plus, la plupart des programmes à télécharger se vérifient au lancement (Ndlr, CRC), et se font revalider par le serveur à chaque connexion (Ndlr, CRC aussi), leurs modifications aussi bien locales que sur le site ne ferait donc que les rendre inutilisables dans le jeu réel. Il faut savoir également que ces programmes ne font qu'afficher les résultats calculés sur le serveur de jeux. Il faudrait donc pouvoir attaquer le serveur de jeux lui-même pour espérer un gain illicite. Pour reconnaître un casino online digne de ce nom, il existe différents labels délivrés par des groupements d'exploitants ou par des sociétés d'audit comme PriceWaterhouseCoopers par exemple. Le problème est de vérifier la validité de ces labels. Actuellement la meilleure méthode semble est de ne faire confiance qu'à des casinos établis depuis plusieurs années ou adossés à des casinos réels.

Que pensez-vous de la position de la Française des jeux sur le sujet des casinos Internet interdits en France ?

Je pense qu'il n'y a pas de réelle concurrence. Il serait simplement grand temps d'autoriser les acteurs déjà implantés à ouvrir des jeux en ligne, car pour l'instant, ils sont en train de se faire prendre le marché par des acteurs à l'éthique pas toujours très développée. La situation actuelle n'a pour effet que de favoriser les casinos en ligne implantés dans des "paradis législatifs et fiscaux", et de faire perdre à la France toutes les taxes rattachées. En revanche l'ouverture du marché aux opérateurs français leur permettrait de gagner des parts de marché hors de France (Ndlr, donc gains de taxes pour la France) et accélérerait la moralisation du marché, l'arrivée de gros opérateurs ayant pour effet d'étouffer les toutes petites structures "exotiques" à l'origine de malversations.

GSM hors service

Nous vous parlions sur zataz.com d'une technique permettant de détruire à distance un téléphone Siemens. La société n'avait pas, à l'époque, souhaité communiquer sur le sujet. Voilà qui est fait aujourd'hui avec une explication du problème. Les ingénieurs de Siemens expliquent que la destruction sous forme d'un Déni de Service, permet de perturber un téléphone Siemens en envoyant un sms mal formé avec un asterix devant le message : *zataz. Jacob Rice, porte-parole de Siemens explique que la gamme S45 ne risque rien, le téléphone peut être relancé après quelques minutes.

Master minding

Voilà qui a de quoi énerver Clain Anderson, un ponte de la sécurité informatique mondiale, responsable de la sécurité client chez IBM. Son fils de 17 ans, Loren, a été arrêté pour escroquerie informatique. Il aurait dérobé pour 100.000 dollars via le vol de numéros de cartes bancaires.

Coup de pouce

Un de nos lecteurs, nous l'appellerons monsieur X, nous a contacté dernièrement après avoir découvert une faille sérieuse dans le site internet de la société Juridis. Cette entreprise est spécialisée dans le recouvrement. La faille ouvrait carrément l'accès à l'administration du site avec informations clients et financières... Bref des données qui n'ont rien à faire sur Internet ! Dès que nous avons eu vent de cette faille, nous avons contacté Juridis pour qu'il corrige. Chose faite rapidement. Tellement vite d'ailleurs qu'ils ont juste oublié de nous remercier. En espérant pour eux qu'aucune information n'aura été volée avant notre alerte...

Le juste prix

Pire qu'un piratage, un bug. Amazon offrait des iPaq H.P. pour 34 euros. Le magazine Branchez-vous explique que durant 15 minutes la version britannique d'Amazon.com a permis d'acheter des assistants personnels iPaq H5450 au prix de 23 livres sterling, soit 34 euros. Le prix de ce genre de "jouet" avoisine normalement les 500 livres, soit plus de 740 euros. Dès la découverte du problème, le site a été fermé pour "problème technique". Les acheteurs qui pensaient avoir fait une bonne affaire ont vu leurs ventes annulées. Amazon expliquant que les ventes ne sont conclues que lors d'une confirmation par e-mail, ce qui n'a pas été le cas.

SACRÉE COQUINE

La grande majorité des Script-kiddies sont des adolescents en mal de reconnaissance. Dès qu'ils peuvent apercevoir une fille sur le réseau, c'est la fête pour eux. Dernière preuve en date ce pirate piégé par une internaute de 15 ans. Le pirate avait réussi à piéger, quelques mois auparavant, une famille britannique. Un trojan dans la machine familiale et le pirate avait eu accès à des informations bancaires qu'il va s'empresser d'utiliser. Bilan près de 3.000 euros détournés. La gamine ne va pas lâcher prise et va draguer l'escroc qui se faisait appeler GafferBoy. Bilan : Le pirate termine en prison.

PROTESTATION

Voilà qui est assez cocasse. Un fan de course automobile de type Nascar, voitures qui tournent en rond à plus de 200 Km/H, a envoyé plus de 530 000 mels à la chaîne de télévision FOX Entertainment. Pourquoi ? La chaîne avait déprogrammé le spectacle attendu par Michel Melo de Billerica, l'internaute mailbombeur, en remplaçant l'émission par un match des Red Sox, équipe de base ball de Boston. Le mécontent vient de plaider coupable devant une cour fédérale. Son action a dû obliger la FOX à fermer son site web entraînant une perte de 36.000 dollars.

LE VIRUS DU PENTAGONE

Le Pentagone a expliqué qu'un pirate a tenté d'envoyer un virus par ses systèmes informatique. Une attaque qui a été contrecarrée avant que le virus ait pu provoquer des dégâts. Le 14 février dernier, un pirate a "spoofé", usurpé, l'adresse du centre d'information des technologies de la Défense (DTIC). Le trasher a camouflé l'adresse réelle de l'émission du virus pour faire croire que l'e-mail portant ce microbe numérique provenait des ordinateurs de Pentagone.

SIR ! YES SIR !

Nous vous parlions en novembre dernier du débarquement du RIAA et de la MPAA au sein de l'école navale américaine. 85 étudiants avaient été épinglés pour avoir téléchargé et diffusé des MP3 et des films pirates. Nous venons d'apprendre les sanctions qui ont visé les marines : restriction d'activités, tours de gardes accrues... Nous sommes très loin des milliards de dollars demandés à d'autres étudiants américains.

ON A RETROUVÉ SADDAM

On n'arrête pas le progrès. Alors que les médias et l'armée américaine recherchent Saddam Hussein, le site de vente aux enchères eBay déborde de produits au sujet de l'ancien dictateur irakien. Des vidéos, des t-shirts, et même le morceau d'une statut de 27 mètres. Ca va faire très joli dans le salon. Il y a de fortes chances que ces enchères ne soient rien d'autre que des tentatives d'escroquerie.

PIÈGE À CON

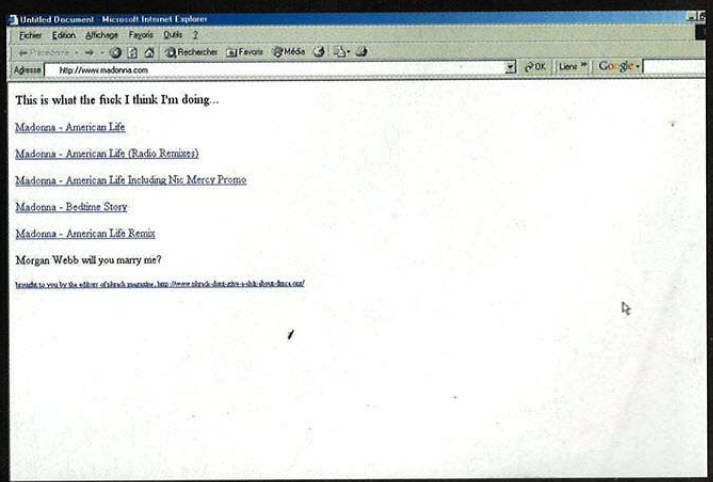
Song-hyun est un étudiant à l'Université de Kyungwon en Corée du Sud. Il a rassemblé près de 90.000 virus depuis 1996. Il a été contacté par une étrange université nommée Mirim College. L'un des chercheurs de ce "college" lui a proposé 100.000 dollars pour sa base de données. Seul hic, la couverture du Mirim College est tombée. Il s'agit en fait d'une structure de l'armée nord coréenne à Pyongyang qui forme des militaires à la cyber-guerre.

LA MADONNE DÉMONIAQUE

Sacrée Madonna. Le moins que l'on puisse dire est qu'elle teste toutes les possibilités pour contrer le piratage de son nouvel album, American Life, sorti en avril dernier. Elle avait annoncé que son équipe avait diffusé des centaines de faux MP3 sur lesquels la chanteuse causait sur la musique.

Côté message "Ce n'est pas bien de copier" ou encore "Quelle mauvaise action es-tu en train de faire". Originale, sûrement efficace et en tout cas collector.

Quelques jours après cette sortie, le site madonna.com a été piraté !

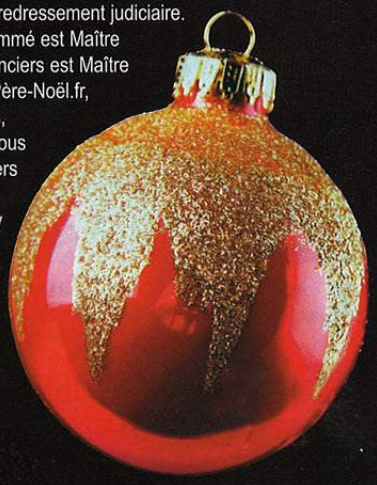


KAZAA, TON UNIVERS IMPITOYABLE

La société Retspan, voir notre interview dans ZATAZ mag 5, s'est spécialisée dans la lutte contre le piratage via des logiciels de type peer-to-peer. Depuis quelques temps des lecteurs nous ont fait part de l'apparition étrange de fichiers appartenant à cette société annonçant "que le piratage ce n'est pas bien". Là où cela devient rigolo, est que ces images apparaissent alors que ce ne sont pas des mp3 ou autres logiciels qui sont en cours de téléchargement, mais des images coquines. Des vidéos auraient aussi été diffusées de la sorte. Du spoofing à partir d'images pour sensibiliser les internautes, en quelques sortes. Madonna a testé ce procédé pour retrouver son site piraté quelques heures plus tard. (Merci à Roy)

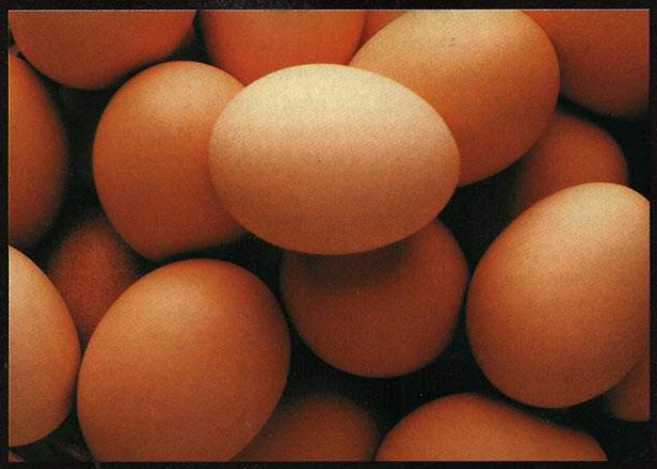
PÈRE-NOËL EN DÉROUTE

C'est le mardi 13 Mai que le tribunal de commerce de Lyon a placé le site de vente sur Internet Père-Noël.fr en redressement judiciaire. L'administrateur judiciaire qui a été nommé est Maître BAULAND et le représentant des créanciers est Maître DUBOIS. Tous les procès civils avec Père-Noël.fr, à l'exception des procès Prud'hommes, sont suspendus jusqu'à ce que vous vous déclariez au représentant des créanciers de Père-Noël.fr, Maître DUBOIS. Attention: il y a une date limite pour s'y déclarer! Faites le donc au plus vite.



TENTATIVE DE PIRATAGE DE NICE PEOPLE

Un clin d'oeil qui nous a amusé : Des personnes ont bombardé le jardin de la villa de Nice People à coup d'oeufs. Une attaque de masse que TF1 ne risque pas de présenter dans ses émissions.

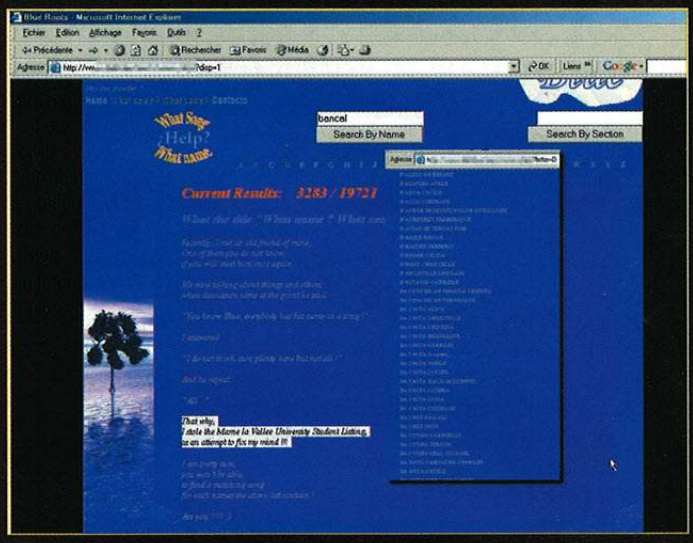


MATRIX RELOADED PIRATÉ

Il y a eu de très nombreux fakes, de faux, du film Matrix Reloaded. Cette fois-ci, malheureusement pour la major, la copie est bien arrivée sur internet. Le groupe pirate, ESOTERiC vient de sortir une version Telesync en deux CDs. Le film a donc été copié via un camescope en salle de projection. Il ne va pas être très difficile de savoir qui est le responsable de cette copie puisqu'il n'y a eu que 3 projections en avant-premières de part le monde.

BASE DE DONNÉES

Les données de l'université de Marne-la-Vallée sont-elles bien protégées ? En faisant une recherche sur le nom de famille Gilles, un de nos lecteurs est tombé sur un site annonçant fièrement que le webmaster avait mis la main sur la liste des anciens étudiants. "(...) I stole the Marne la Vallee University Student Listing (...)". Nous avons contacté l'université en question en attendant une réponse de leur part.



DÉBANDADE

Un homme qui a violé la loi britannique sur les médicaments vient de voir son appel rejeté. Le tribunal de Stafford l'avait condamné en novembre dernier à un an de prison, dont 6 mois ferme pour avoir vendu du Viagra sur Internet sans autorisation. Il a été aussi condamné à 630 000 livres sterling, 880 258 euros, d'amende et à rembourser les 12 500 livres, 17 465 euros, de frais d'avocats des plaignants.

STEGANOPORNO

Le New York Post vient d'expliquer dans ses colonnes que des terroristes italiens du réseau Al-Qaeda auraient utilisé la stéganographie pour cacher des informations dans des images pornos. Ils auraient d'ailleurs été arrêtés grâce à ces images au format jpg. L'affaire a été révélée à Milan, lors du jugement des membres de ce groupe terroriste. Les membres de cette section ont utilisé des images pornos, mais aussi, des photographies du président Bush, du secrétaire d'état Colin Powell ou encore du leader palestinien Yasser Arafat. Après les attentats du 11 septembre, des rumeurs avaient été lancées sur le fait de l'utilisation de stéganographie par Al-Qaeda, sans que le FBI puisse en apporter la preuve.

PORNOGRAPHIE, ARNAQUE

QUEL EST LE MOT LE PLUS TAPÉ DANS LES MOTEURS DE RECHERCHE ? MP3 ? NON ! WAREZ ? NON PLUS ! SEXE. TOUCHÉ ! ON PARLE DE 100 MILLIONS DE PETITS DOIGTS CHERCHANT FRÉNÉTIQUEMENT LES GROS TÉTONS NUMÉRIQUES. ZATAZ MAGAZINE VA VOUS MONTRER QUE LE POINT G, VOUS RISQUEZ DE VOUS LE PRENDRE EN PLEINE TÊTE !

SEXE, MENSONGE ET VIDÉO

Les sites pornos pullulent sur le réseau. Ils sont tous à promettre gratuité, gros nénés et blondinettes déchaînées. La vérité est beaucoup plus glauque que ça encore. Au premier abord, il y a très peu de retenue dans les pages d'accès publique de ces sites pour adultes. Il faut vendre et les premières images doivent accrocher le client potentiel.

Et les mineurs dans tous ça ?

La grande majorité des administrateurs de sites pornographiques ont l'air de s'en moquer comme de leurs premiers boutons d'acné. Il faut certes être majeur pour accéder aux photos, vidéos, chats et autres spécialisations kamasutresques, mais les pages publiques, les vitrines commerciales de ces sites, elles sont hards, très hards et nombre d'enfants tombent dessus. Certaines pages annoncent "gratuité" des documents, mais pas la gratuité de l'accès.

Finalité : Pendant que l'internaute s'astique la souris, les sites pornos pénètrent dans son porte-monnaie. En France, les tribunaux n'ont pas de pitié pour ce genre de comportement. Un exploitant de sites Internet pornographiques, a été condamné le 2 avril à 30 000 euros d'amende par la cour d'appel de Paris pour ne pas avoir instauré un système efficace d'interdiction d'accès aux mineurs. La cour d'appel a doublé la peine décidée en première instance par le tribunal de grande instance de Paris.

"Les mises en garde et informations sur les logiciels de restriction d'accès présentées dans les pages d'accueil (...) ne sauraient être considérées comme des précautions utiles puisqu'elles interviennent alors que l'utilisateur est déjà entré dans le site et n'empêchent nullement la vision des textes et photos de présentation (...) Il appartient à celui qui décide à des fins commerciales de diffuser des images pornographiques sur le réseau Internet dont les particulières facilitées d'accès sont connues, de prendre les précautions qui s'imposent pour rendre impossible l'accès des mineurs à ces messages."

Un site comme tant d'autres consacrés aux mots de passe de sites pornos.

Les boards sont une mine d'or pour ceux qui recherchent des accès dérobés

PIRATES ET SÉSAMES MAGIQUES

Des petits malins, adeptes des dessous roses, se sont spécialisés dans le piratage de sites pornos.

L'idée : rendre gratuit les accès aux sites pour adultes.

Et si le petit frère tombe sur ce genre de chose ? Xenon, l'un des pirates spécialisés dans le porno que nous avons rencontré pour cet article nous explique : "Il faut pas se voiler la face. Les 16-18 ans sont les premiers clients de ce genre de sites. Comme nous n'avons pas d'argent et pas de moyen d'accès légaux, il faut s'ouvrir des portes... par derrière."

Comment agissent-ils ? Malheureusement très simplement, souvent au grand dam d'internautes n'ayant rien demandé, ou presque. "Je me suis spécialisé dans la base de données de cartes bancaires sur site porno. Je m'arrange pour récupérer plusieurs numéros bancaires validés par de vrais clients sur un site porno X que je vais réutiliser pour ouvrir des accès "gratuits" sur d'autres sites pornos" dixit @rob@z, autre pirate spécialisé dans le Hack'porno. Du vol pur et simple "Oui, il faut l'admettre, mais les clients qui ont été s'abonnés voient rarement la différence et surtout ne vont pas oser se plaindre... du moins tout suite." Les logins et mots de passe sont ensuite redistribués dans des boards, des forums, des chats IRC, des sites web. Facilement détectable par les administrateurs comme nous l'a expliqué Laurent C. gestionnaire d'un portail porno en Italie : "Je tourne beaucoup sur certains chans pirates. Ils balancent les url des sites piratés. Je regarde si les sites dont j'ai la gestion s'y trouvent. Il ne me reste plus qu'à couper les comptes créés par les pirates". Et à la question de savoir s'il profite de ce genre de promotion, il nous répond :"J'avoue qu'il m'arrive de balancer quelques faux comptes pour faire venir le chaland. Une fois sur le site il est assommé de publicité. Ca rapporte". L'internaute noyé par la publicité quand ce n'est pas son navigateur qui est phagocyté par le site porno lui-même.

S, SPAM ET COMPAGNIE

VIRUS, SPAMS ET ESCROQUERIES

La grande mode pour beaucoup de sites pornographiques est de squatter les options des navigateurs, Internet explorer en tête. Comment ? Simple comme un bug de I.E. Les sites pornos cachent en leur sein un code malveillant exploitant un bug dans l'applet ActiveX incitant ainsi les navigateurs à mettre dans l'option "Démarrage" de la machine de l'internaute l'url du site visité. Et encore, ici nous parlons de l'exploit le plus soft utilisé par les sites pornos. Certains n'hésitent pas à faire de manière à ce qu'à chaque connexion de la machine, l'utilisateur se retrouve avec des dizaines de publicités qui vont s'afficher à l'écran. Imaginez l'ambiance, le matin, au boulot. Déjà que nos boites de courriers électroniques sont envahies de messages !

Certains sites pornos se sont même d'ailleurs trouvés un bon plan à spam. Ils créent des sites anti-spams afin de récupérer des adresses e-mail qui serviront à des publicités non sollicitées pour des sites de cul.

Voici un exemple vécu par un de nos lecteurs : "Je reçois depuis plusieurs jours dans ma boite des e-mails assez lubriques se finissant tous par l'adresse www.remove-yourself2.com . Bien décidé a mettre fin à cela, je me rends sur le dit site. Qui se trouve en fait être à cette adresse : http://www.REMOVE-YOURSELF2.com @www.mrspanky.com/removeyourself2/remove.php. J'envoie un mail à Questions@MrSpanky.com en lui demandant de me retirer de sa liste. Je reçois un mail me disant que cette adresse n'est pas valide. Par curiosité je fais un ping -a www.mrspanky.com puis un ping -a adresseIP-du-site-mrspanky, et, surprise, je tombe sur newvhost.siscom.net qui se révèle être un site anti-spam." Un site dédié à la lutte contre le spam utilisé par un site pornographique pour envoyer du courrier afin de spammer les boites aux lettres d'internautes. Faut être tordu quand même !

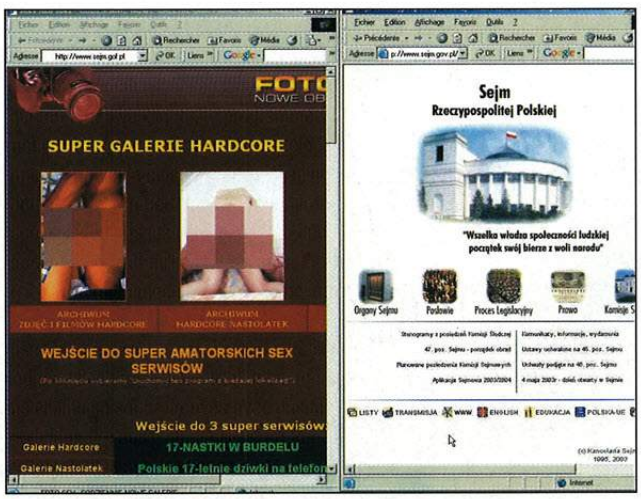
Dernière grosse arnaque du genre, les kits de connexion. De plus en plus de sites à l'étranger, car les kits de connexions sont théoriquement interdits en France, annoncent la gratuité de leur contenu. Pour cela, il faut juste télécharger un petit programme bien anodin. L'internaute qui possède encore un modem 56K n'y verra que du feu. Il va cliquer, le programme va le déconnecter d'Internet pour le renvoyer sur une ligne téléphonique surtaxée, pouvant coûter jusqu'à plusieurs euros la minute. Là, croyez-nous, la débandade de votre portefeuille va se faire sentir. La société Verity, spécialisée dans les sites pornos, a dû faire une croix sur la bagatelle somme de 1.6 millions de dollars. La Commission Commerciale fédérale américaine lui a proposé de rendre l'argent plutôt que de se voir poursuivie pour fraude et utilisation de connexions malhonnêtes. Un cas d'école cette société ! Elle avait incité les mateurs à télécharger un logiciel qui rendait payant les sites visités. Certains clients se sont retrouvés avec des factures avoisinant les 4.000 dollars. Il faut dire aussi que la filiale de Verity, eBillit, renvoyait les internautes sur des lignes au Madagascar à 4 dollars la minute.

France2, une autre idée du service publique...

Nous ne pouvions pas finir cet article sans parler des faux sites, des squatters de noms de grandes marques. Nous avions été les premiers, début 2001, à découvrir qu'un webmaster italien de sites pornos, Augusto Verzetti, avait squatté les noms de domaine de chaînes de télévisons françaises : france2.com, france3.com, france3info.com... Aujourd'hui certains de ces sites sont passés dans l'escarcelle de sites pornos coréens.

En attendant, notre italien possédait aussi lacinquieme.com, cinecinema1.com, cinecinema2.com, mangas.com, rtltelevison.com, rtltv.com, telemontecarlo.com ou encore tv5europe.com. Le dernier cas en date, qui pourrait prêter à sourire vise le gouvernement polonais. L'agence polonaise de protection des consommateurs vient de mettre en garde les internautes du pays après la découverte d'un faux site du gouvernement, www.sejm.gof.pl, qui à défaut de présenter lois et comptes rendus politiques affiche du contenu porno. Les pirates ont profité du fait que le .gov, signalant un site du gouvernement, soit proche du .gof, qui a été utilisé par le site pour adulte. Le webmaster n'a pas hésité, dans la foulée, à utiliser une faille d'Internet

A droite un site gouvernemental polonais officiel, à gauche, son pendant porno...



WESTERN UNION FRÔLE LE DÉSASTRE

UN HACKER BLANC FRANÇAIS A SAUVÉ DES PIRATES LES COMPTES DE PLUSIEURS MILLIONS DE CLIENTS DE LA BANQUE WESTERN UNION. VOICI CETTE HISTOIRE, DIGNE D'UN FILM D'ESPIONNAGE, UNE EXCLUSIVITÉ ZATAZ MAGAZINE.

PROMENADE SUR LE WEB

Notre hacker blanc, nous ne citerons pas son identité, a découvert mi-mars, lors d'une visite sur Internet un problème de sécurité incroyable chez la banque Western Union. Lors d'une cession Telnet, sa machine va lui envoyer comme information une connexion sur une adresse IP demandant un login et mot de passe.

Classique, un message d'alerte apparaît à l'écran : "Connected to 206.201.228.2" suivit d'un "User Access Verification - Username:admin - Password: - Notre hacker blanc, professionnel de la sécurité informatique, ne sait pas encore qu'il a affaire avec un serveur de la Western Union. Il se penche donc une seconde sur cette demande de mot de passe. Par pur réflexe, il saisit "admin" et ...

SÉSAME OUVRE-TOI

C'est un français qui a sauvé la mise de la célèbre banque américaine.

... et l'accès à la machine s'ouvre sans autre demande. Intrigué, notre White Hat commence à se poser des questions: Qui se cache derrière cette machine aussi peu protégée ? Sans doute encore un particulier qui a oublié de mettre en place sa propre protection, laissant la configuration sécurité de base installée par le constructeur. Notre hacker blanc va donc se rendre sur notre site, dans notre option "tracer infos", afin de connaître le propriétaire de cette adresse IP. Le whois, la carte d'identité du propriétaire va lui apparaître et quelle ne fût pas sa surprise de tomber sur un serveur de la banque américaine Western Union ! Le serveur découvert par ce White hat n'est pas inutile. Il a pour mission du faire du "load balancing", comprenez de la répartition de charge entre deux firewalls de cette société. Un problème de mot de passe pour une banque, de quoi s'inquiéter surtout qu'ici le problème aurait pu être très simplement corrigé. Il suffisait de lire la notice et de modifier le login et le mot de passe installé par défaut, le trop célèbre admin/admin. Imaginez que notre hacker blanc fût plutôt un pirate, il serait devenu administrateur sur cette machine, un bon gros Cisco CSS 11050.

QUEL RISQUE ?

Accès au serveur comme administrateur, donc comme le responsable de ce serveur, machine ayant gestion des firewalls, Pas besoin d'en dire plus.

Le risque était énorme comme par exemple pouvoir sniffer le trafic et d'utiliser la boite comme un proxy. Ici le pirate aurait pu se servir de cette connexion comme d'un rebond pour un autre piratage. Pire, envoyer des informations sous le nom de la Western Union. Un problème de mot de passe, malheureusement fréquent notamment dans des milieux professionnels ou l'informatique n'est pas le corps de métier principal. Notre White hat ne tournera pas sa souris sept fois sur son bureau. Il va contacter la banque qui va lui répondre en moins de 24 heures. Aujourd'hui plus de problème pour les millions de clients de cette banque, l'adresse IP affiche aujourd'hui un fier et robuste : "System unavailable. Please try later. Connection closed by foreign host."

Les articles - en anglais - au sujet des pirates ayant touché la Wester Union.
http://www.washingtonpost.com/wp-srv/aponline/20000910/aponline195401_000.htm
http://www.westernunion.com/info/privacyPolicy.asp
http://zdnet.com.com/2100-11-523769.html?legacy=zdnn

NOUVEAU ?

Pas vraiment, les banques sont des cibles privilégiées par certains pirates plus proche des groupes mafieux que du petit script-kiddy en mal de reconnaissance. Pour la Wester Union, les tentatives de piratages sont légions. Tous ne sont pas connus, d'autres oui. Début septembre 2000, la banque basée à Boston confirmera le vol des informations bancaires de 15.700 de ses clients. Le pirate avait transféré de l'argent alors que l'un des serveurs de la Western n'était pas protégé en raison de la maintenance de ce dernier. Cette banque qui a connu les cow-boys lors de sa création en 1871 n'a pas fini de voir passer les bandits de grand chemin.

LA DÉFERLANTE FRANÇAISE DES BOARDS WAREZ PAR CNS

Vous avez été très nombreux à réagir à propos de l'article publié dans le numéro précédent de Zataz, qui traitait des Boards Warez. Et d'après vous, il n'existe pas tant de boards que ça sur Internet. Nous nous sommes donc penchés sur le sujet en cherchant sur le réseau, le nombre de boards existant en France. Voici, en images, notre pêche miraculeuse. En raison du manque de place sur cette page, d'autres captures sont publiées mag.zataz.com . Le résultat est en tout cas plutôt éloquent : il existe des boards warez en France, et beaucoup de surcroît !

Les boards sur le web sont légions. Des dizaines de lieux où s'échangent serveurs, logiciels, musiques, films piratés. En voici une liste non exhaustive : Adk ; Activeteam ; Akg ; Amnesik ; Alliance ; AnarchyBoard ; Apparence ; Arkadia ; Atlantide ; Atlantis ; Atomik ; Azazell ; Bhz ; Babivanille ; Black and white ; Betasfrench ; Burst ; Burger ; CbwarezS ; CRS ; CoolBytes ; CoolOnly ; Crazy Cliqueur ; Dcdream ; DPC ; Dagoboard ; Dignity ; Dragon Sanctury ; Dream Team ; Eden ; Elemental ; Eliteam ; Ex0dus ; Exception ; Evoluted ; Eternity ; FSB-Team ; Fire-Board ; Floppy ; Gaia ; Genesis ; H2O ; HHC ; Heaven ; HuuH ; Homer ; Hydrogène ; Infernal-Team ; Inside ; Illegal ; Infinite ; JPL-team ; KAOSS ; K-ribou ; Le souk ; Legend ; LiThiuM ; LoL ; Logiteam ; Looney Board ; Maniac ; Magical ; MB ; MessiaH ; Mojito ; Monk ; MDR ; NBG ; NastyFXP ; Nemesis ; NeRD ; Obione ; Ogay ; OmegaBoard ; Opak ; Osiris Clan ; Oxyd ; Oxyde ; Pacifik ; Paradiv-x ; Paradise ; Panik ; PDF ; Pixel ; PoussinWarez ; Profuzion ; Ps2FXP ; Remi ; Rebirth ; Rescue ; Revelation ; RedZone ; RoccoBoard ; Savuka ; Sprit3 ; Serenity ; Sequence ; Sitateam ; S-Kro ; SteaM ; Squeeze ; Skwaterz ; Snowboard ; Solarus ; Spartateur ; Sphere ; Spider ; SuspectFXP ; Symbioz ; T-Phoenix ; Tengoku ; The indians ; The lost team ; Toxic ; TNG ; TitanFXP ; Twilight FXP ; Ulysse ; UniTy ; Universal-DivX ; Vertical ; Versatil ; Vibe ; Viper ; Vip-Board ; QiX ; WF@dsl ; WsC ; WaX Crew ; Wanted ; Weed Board (WBC) ; Wizard Board ; Xpression ; XtremBoard ; ZCE ; ZwB

MARC HENAUER : JE SUIS UN CYBER POLICIER

C'est à l'initiation de l'Internet Society et du club de la presse de Genève que nous avons rencontré Marc Henauer de l'Office fédéral de la police suisse. Ce cyber-policier travaille pour le service national de coordination de la lutte contre la criminalité sur Internet. Nous en avons profité pour lui poser quelques questions sur ce nouveau service créé en janvier 2003.

Qu'est ce que le SCOCI ?

Le service national de coordination de la lutte contre la criminalité sur Internet est un service de police centralisé pour les personnes souhaitant signaler l'existence de sites Internet suspects. Nous recherchons des contenus illicites sur Internet et nous avons une mission de renseignement et d'analyse dans le domaine de la criminalité sur Internet. La cellule recherche les indices à travers Internet, nous vérifions ensuite si l'objet litigieux a un rapport avec la Suisse et s'il viole le droit helvétique. Si cela est le cas, nous transmettons le dossier aux juges d'instruction. Si le cas ne vise pas directement la Suisse, le dossier est diffusé à nos homologues via Interpol par exemple.

Pourquoi un tel service ?

Nous savons qu'il existe une communauté underground, certains font des choses illégales nous sommes là. La Suisse est un pays fédéral, avec 26 corps de police par canton, 26 polices avec compétences d'enquêtes. En suisse nous n'avons de FBI, donc si nous avons un problème avec un pirate dans un canton, vers un autre canton, nous nous retrouvions avec deux corps de polices pour le même sujet, d'où problème. Il y avait un gros souci coordination, d'où la création de notre service contre la criminalité sur Internet. Un petit service de 8 personnes pour le moment qui coordonne les actions. Un monitoring des actes sur le web suisse.

Le dialogue avec la communauté underground semble être quelque chose d'important pour le SCOCI, pourquoi ?

On peut faire ce travail de recherche, de monitoring, sans le dialogue avec les hackers, la communauté underground. Mais pour nous nous pensons que le dialogue est très important parce que nous sommes certains que la communauté travaille à fixer les problèmes plus qu'à en créer. D'où l'importance du dialogue, notre cellule technique permet ce dialogue. Notre système est proche de celui qui est utilisé dans certains hôpitaux. Dès qu'une information arrive, elle est diffusée aux bonnes personnes. Par exemple des qu'un site apparaît et qu'il rentre dans nos critères il est sauvegardé, analysé et si besoin un renseignement plus poussé sera lancé.

L'internet, vrai problème ?

Notre mission est de faire en sorte que l'internet ne soit pas une sphère sans loi, anarchiste. Ce n'est pas un jardin d'enfant, donc nous nous devons d'être là ! La Suisse a agit car il y avait un vrai manque de communication et le laissé faire n'est pas possible. Le déclic a été la pédophilie sur Internet. Notre ministre de l'Intérieur a été le moteur pour notre équipe.

Comment agissez-vous par exemple pour les mels ?

En suisse les mels sont traités comme des télécommunications. Et comme les télécommunications les mels sont gardées pendant 6 mois, nous n'enregistrons pas les conversations, le contenu, mais il y a obligation de garder les dates d'envois de ces derniers. Il est possible s'il y a enquête, de mettre sur écoute. Mais nous ne le ferons pas sans un accord d'un juge. Nous ne sommes pas Big brother. Le processus démocratique est respecté. Nous n'agissons pas sans l'accord d'un juge.

Etonnamment votre service différencie bien le pirate du hacker.
Nous avons fait une classification que nous trouvions importante. Nous faisons la différence entre un hacktiviste, un pirate, un script-kiddy,... Pour la police, nous faisons certes la différence, mais au vu de la loi l'acte est le même. Notre rôle n'est pas de trouver un pirate et de l'arrêter. Nous avons une action de communication, information, renseignement.

Vos moyens ?

Nous sommes pour le moment huit. Nous avons des systèmes qui permettent de faire un monitoring efficace. Ils permettent de regrouper des informations précises. Nous avons des outils qui automatisent certaines choses. Mais la main humaine reste indispensable. Nous avions prévu 3 000 alertes par année. Nous sommes à quasiment 2 000 alertes en à peine 6 mois. Dès qu'une alerte est lancée, nous agissons. Analyses, renseignements, classifications...

Des cas rencontrés de cyber-délits

Un exemple, le cas de fausses écoles privées suisse hôtelière. Notre pays est connu pour la qualité de ses formations en hôtellerie. De faux sites sont apparus en Chine vantant des écoles fictives qui ont attiré des étudiants qui se sont fait piéger et qui ont payé.

La Suisse possède d'étranges photocopieurs publics contenant des disques durs, pourquoi ?

Je ne suis pas au courant de cette chose. Je suppose que cela a pour but de contrer les faussaires, les copieurs de billets de banques...

DES INFORMATICIENS POUR AIDER LA POLICE

Cedric Renoir est ingénieur chez Ilion security. Cet informaticien de talent est spécialisé dans les testes d'intrusions. Ses clients, les banques suisses. Il forme aussi policiers et magistrats à comprendre qui sont les hackers, pirates et compagnies. - ilionsecurity.ch -

Quel est votre rôle auprès de la police ?
On s'occupe, entre autre, de former des policiers et des magistrats. On les initie aux intrusions informatiques, non pas pour en faire des pirates mais pour qu'ils comprennent et deviennent des gens compétents. Ils seront ensuite capables de comprendre les liens entre les méthodes des pirates et les réseaux criminels économique classique.

Vous leur apprenez quoi ?
On leur apprend qui sont les hackers, les pirates, les script-kiddies. On leur montre les outils et les méthodes des pirates : Virus, cheval de Troie, brute force cracker... On organise des séances de démonstrations. On leur montre les risques. Le but étant de leur montrer quoi faire, quel expert appeler et surtout savoir lire un rapport d'expert.

Que pensez-vous de cette démarche qui est d'écouter et comprendre la scène underground informatique ?
La démarche en suisse est excellente car nous avons des interlocuteurs. Il y a un vrai besoin de compréhension et c'est la seule manière qui puisse faire progresser les choses sans être obligé de mettre en place des lois liberticides comme dans certains pays. Ce n'est pas en assenant un grand coup de massue sur les gamins qui sont attrapés. Ils doivent être punis mais sans les assommer. Cette méthode ne permet pas de toucher les "gens" réellement compétents. Mais l'écoute, la compréhension et la coopération permet de punir uniquement ceux qui en valent le coup. Qui causent de vrais dégâts ? En formant ces policiers et magistrats cela permet de les sensibiliser au problème.

MICROSOFT MAÎTRE DU MONDE ?

En 1975 un jeune américain lance son projet qui est de rendre l'informatique accessible à tous. 1983, ce projet débarque en France sous le nom de Microsoft. Depuis cette date, qui n'a jamais utilisé Windows, Word, Excel ? Qui n'a jamais entendu parler de Bill Gates ? Microsoft est depuis pr{ès} de 20 ans l'entité informatique qui domine de la tête et de la souris le monde informatique. Nous avons rencontré Christophe Aulnette, le directeur général de Microsoft France, pour parler un peu de ce géant pas comme les autres.

Microsoft est certes le leader du marché du logiciel informatique mais fait partie aussi des plus attaqués. On lui reproche son monopole, ses problèmes de sécurité... Christophe Aulnette ne va pas contredire cet aspect et ne va pas hésiter d'ailleurs à admettre quelques erreurs de jeunesse. "Nous n'étions pas parfaits mais nous avons fait de sérieux progrès". Il faut dire aussi que le nombre de problèmes de sécurité visant les produits Microsoft sont pléthores et ne laissent pas indifférant l'utilisateur confronté à un virus, voir plus dommageable encore, à un pirate. "Depuis 1 an 1/2 nous avons mis en avant l'informatique de confiance. C'est une question d'équilibre. Nous avons mis en place par exemple des outils comme l'Update qui permet de recevoir les patchs de sécurité sans être dérangé durant son travail." Une mise à jour d'ailleurs qui inquiète. "Il est vrai que nous devons améliorer notre communication. Si l'utilisateur nous remonte des problèmes, nous nous devons d'expliquer l'utilisation des informations que nous avons reçues."

La transparence chez Microsoft, un nouveau cheval de bataille ?

Elle prend d'ailleurs une forme très étonnante via la fourniture du code source des logiciels et plus précisément des OS Windows 95, 98, Me, 2000, NT, XP et même de la version bêta de Windows 2003 et Windows CE pour pocket PC et autres téléphones mobiles. Une 20ène de DVD, d'après Guillaume Tourres chargé de projets chez Microsoft France. La Russie et la Chine ont été les premiers à avoir répondu présents. Des contacts en France sont en cours. La prise de conscience des enjeux de sécurité informatique fait donc son chemin. "Même si nous avons toujours été très soucieux de la sécurité. Aujourd'hui nous avons mis les bouchers doubles pour que cela soit plus efficace."

Palladium, big brother ?

Et l'avenir ? "Office 2003, Windows server 2003, Palladium, et nos 20 ans que nous allons fêter en juin prochain". Des avancées significatives pour les utilisateurs ? Attendons de voir. Nous avons d'ailleurs posé la question au sujet du problème que pose le XML dans les futurs produits Microsoft. Language qui inquiète sévèrement les antivirus. "Nous sommes très fiers de XML. Nous nous sommes engagés autours de ce standard. La réflexion de sécurité a été importante à ce sujet et nous n'avons pas de crainte". A noter d'ailleurs que Microsoft France vient de créer une fonction de - Chief Security Officer - qui sous l'égide de Bernard Ourghanlian a pour but de concevoir, piloter et animer les actions dans le domaine de la sécurité informatique. "Nous nous devons de contribuer à assurer la sécurité d'Internet et des données de nos clients".

Les rumeurs sur le futur Windows, nommé Palladium a déjà fait beaucoup couler d'encre sur son aspect intrusion dans la vie privée. "Beaucoup de fantasme autours de Palladium. Nous n'avons fait que récupérer des informations techniques pour avoir une idée des possibilités et rien d'autre. Notre but n'est pas de surveiller mais de s'assurer que les particuliers et les entreprises pourront se sécuriser de manière efficace. Pas question pour nous de nous initier dans la vie privée des gens sous prétexte de sécurité. On nous a jugé avant même d'avoir testé le produit."

Microsoft vs Linux

Les anti-Microsoft ne sont pas légions mais existent et le font savoir. Nous avons donc posé quelques questions aux sujets de linux et de l'Open-source, le GPL, la distribution gratuite et alternative de logiciels informatiques. "Une très bonne idée, mais je doute qu'à long terme on soit dans le même état d'esprit. Ca génère du service plus qu'un logiciel packagé comme Microsoft et donc à la longue c'est plus coûteux. Une chose est certaine, Linux est un concurrent nouveau et sérieux." A notre question sur le GPL, la licence libre, la réponse de Christophe Aulnette sera sans appel : "Le GPL c'est nier la propriété intellectuelle. Philosophiquement je trouve cela très dangereux. La propriété intellectuelle génère création et innovation."

Microsoft semble se porter à merveille, tant mieux pour eux, tant mieux pour les millions d'utilisateurs. L'avenir nous dira si la correction et la compréhension des erreurs du passé vont être profitables pour tous.

FAUT-IL AVOUER PEUR DE PALLADIUM ?

Microsoft est en train de préparer un ordinateur révolutionnaire. Le système va se nommer Palladium. Un ensemble de techniques dans une même machine capable de crypter les données, protéger des pirates, des virii et surtout, protéger les sociétés commerciales afin d'éviter l'utilisation ou la diffusion de copie. Fusionner avec le Passeport de Microsoft qui va permettre d'enregistrer à vie nos informations privées et/ou professionnelles afin de nous faire gagner du temps. Fusionner tout cela avec le disque dur virtuel que va offrir Microsoft, le MyLifeBits, qui va permettre de sauvegarder toutes nos informations numériques directement chez Microsoft, on peut effectivement s'inquiéter de cette main mise numérique de nos vies par la firme de Bill Gates. Gordon Bell, le concepteur du programme MyLifeBits le dit lui-même.
« Il existe un réel danger si un pirate arrive à se connecter à cette base de données géante ».

CARTE DE VISITE

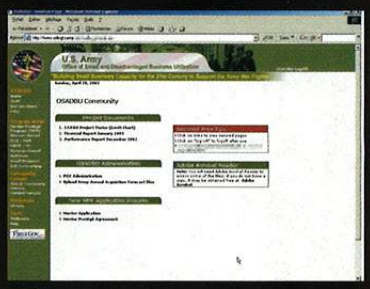
Directeur général France depuis 2000, vice-président Microsoft Europe/Moyen-Orient/Afrique, Christophe Aulnette a débuté chez Microsoft en tant qu'ingénieur commercial. Il a connu les débuts de l'informatique, de Windows et des logiciels qui vont en découler. Passé par Microsoft Asie, via Singapour et Tokyo, il est aujourd'hui en France à la tête de 950 salariés. Il définit sa mission comme "la gestion d'une grosse PME". Et quelle PME. Plusieurs centaines de produits dont certains devenus quasiment indispensables. Windows pour n'en citer qu'un. Logiciels commercialisés via 4000 partenaires sur tout le territoire.

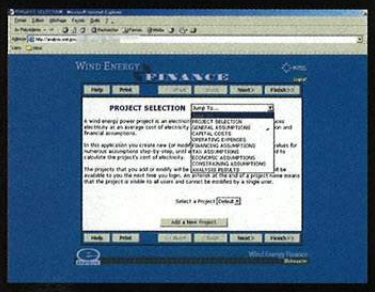
WAR GAMES

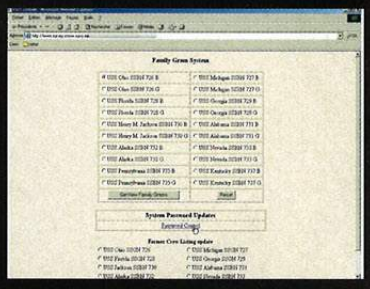
Les sites militaires américains sont-ils tous ultra protégés ? D'après la Maison Blanche, les pirates se casseront les dents à tenter une percée. ZATAZ Magazine va vous montrer que certains serveurs de l'armée de l'Oncle Sam sont malheureusement ouverts à tous les vents. Exclusif !

MY NAME IS JOSHUA

Certains magazines ont titré dernièrement sur le fait que les sites militaires américains étaient faillibles à des problèmes de CSS. Pas vraiment des failles, plutôt de petits problèmes de conception qui ne risquent pas de faire grand mal. Nous, nous allons vous montrer des choses plus sérieuses, plus inquiétantes surtout. Si le problème de CSS permet de jouer avec un url, nos découvertes à nous permettent 10.000 fois plus de choses, et pour cause, elles ouvrent les portes des administrations des sites militaires que nous avons trouvés. Ce qui nous a motivé à écrire cet article fut le commentaire du Ministre de la défense nationale américaine, Donald Rumsfeld. Il a ordonné début janvier 2003 aux militaires de vider leurs sites d'informations qui pourraient être utilisées par des terroristes. Le ministre s'était inquiété après la découverte, en Afghanistan, de matériel informatique contenant pas moins de 700 Giga octets d'informations récupérées sur le web par un membre d'Al-Qaeda.

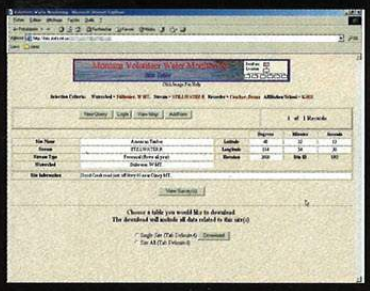


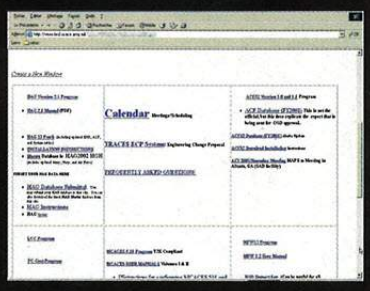




UNCLE SAM

Nous vous en parlions il y a plus d'un an, le moteur de recherche Google possède une option particulière. En tapant google.com/unclesam/ l'internaute curieux se retrouve avec un moteur de recherche offrant uniquement des liens et documents du gouvernement américains. Notre enquête est partie de cet url. Nous nous sommes contentés de taper ".mil", comprenez, tous les sites militaires américains. Durant une semaine nous avons cherché, regroupé, trié et découvert pas moins de 260 sites militaires américains dont la sécurité était proche de zéro. 95 % de ces sites possédaient bien un accès login et mot de passe, seulement les administrateurs semblent avoir des lacunes avec leurs mises à jour. Tous avaient oublié de patcher la faille Bypass SQL.





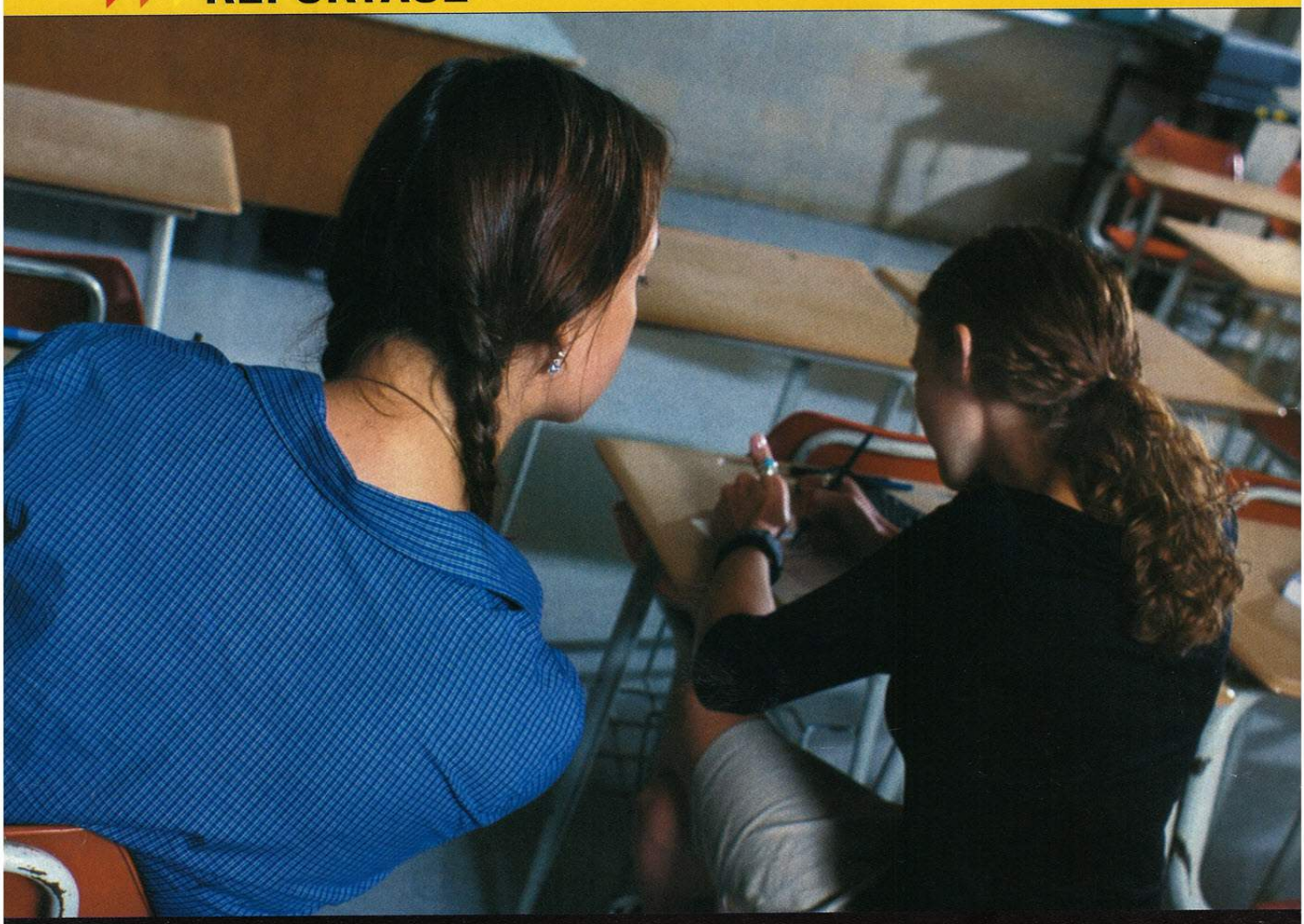
PÊCHE MIRACULEUSE

Les sites que nous vous présentons dans cette page sont des sites militaires ou du gouvernement américain. Gestion des fichiers, des comptes membres et d'informations, modifications d'infos et de mots de passe, gestion de l'eau du Montana... De quoi se faire passer pour un responsable de sites militaires, récupérer des informations qui ne devraient pas être aussi faciles d'accès. Comme vous avez pu le voir, pas la peine d'être un super méchant pour tomber sur des documents qui peuvent être considérés sensibles.

TOC ! TOC ! TOC !

Imaginez : l'Oncle Sam a fait les gros yeux en janvier dernier. Il estime que les sites du gouvernement américain doivent être protégés et ne plus laisser de possibilité de regarder, lire, ce qui doit rester dans les bureaux. F.a.b., un lecteur de ZATAZ Magazine, nous a fait parvenir une astuce qui nous a laissé pantois. Grâce à Internet explorer et à une option du navigateur de Microsoft il est possible d'accéder aux informations du FTP de certains sites du gouvernement américain. Notre capture écran concerne le site cwc.gov mais sachez que nous avons eu accès aussi à des sites encore plus sensibles comme Navy.mil, ... Dans certains cas il était carrément possible de télécharger sur le serveur des données. Il va falloir que l'Oncle Sam face réviser ses administrateurs.

Accés au serveur de ce site du gouvernement US uniquement avec I.E.



TRICHER AUX EXAMENS!

Depuis que l'école et les examens existent, il y a toujours eu un camarade prêt à tout pour ne pas bosser ! Potasser les examens ? Il n'a même pas ces mots dans son vocabulaire.
Lui son truc, c'est réussir en trichant. Nous avons donc sorti notre sac à provision pour voir ce qui existait en ce moment sur le marché pour tricher à la sauce high-tech. Edifiant !

EXAMEN DE GÉOGRAPHIE

Avec la révolution GSM, iMode et compagnie, les téléphones mobiles ont plus l'air de tableaux de bord multifonctions que de simples boites servant à appeler ses potes pour boire un coup ! Beaucoup de petits malins ont d'ailleurs compris le truc. De nombreux téléphones offrent la possibilité de faire du wap, et autres. "Nous avons mis en place des sites antisèche" dixit l'un de nos correspondants. Investissement minime vu les packs proposant un téléphone multimédia. Pour les plus riches, le téléphone Suunto, couplé avec un GPS et les cartes qui vont avec sera le must pour la géographie.
Seul petit frein, le prix, proche de 1 000 euros.
http://www.navicom.fr

EXAMEN D'HISTOIRE

Avec la mode du MP3, il existe des dizaines d'objets permettant d'enregistrer les cours d'histoire, qu'il ne vous reste plus qu'à diffuser via un mini casque. Simple comme bonjour, des montres, comme la montre Wrist audio MP3, premier lecteur audio MP3 miniaturisé. Prix : 299 euros.
Dans un autre genre, le briquet MP3. En fait, une clé USB Pen Drive MP3 qui permet de mettre en mémoire 128 Mo

de citation en tout genre. Prix : 99 euros. Dans un autre genre, l'antisèche visuelle via des photographies intégrées dans votre montre. Petit bijou du genre, la Casio WQV-10J, avec un écran LCD de prévisualisation en couleur. 100 photos possibles en mémoire, port infrarouge entre la montre et un PC. Prix aux alentours des 300 euros. La loupe n'est pas fournie avec.

http://ldlc.fr/fiche/PB00016186.html
http://www.inet-time.fr/innovationmp3casio.htm
http://www.canon.com

EXAMEN DE LANGUES

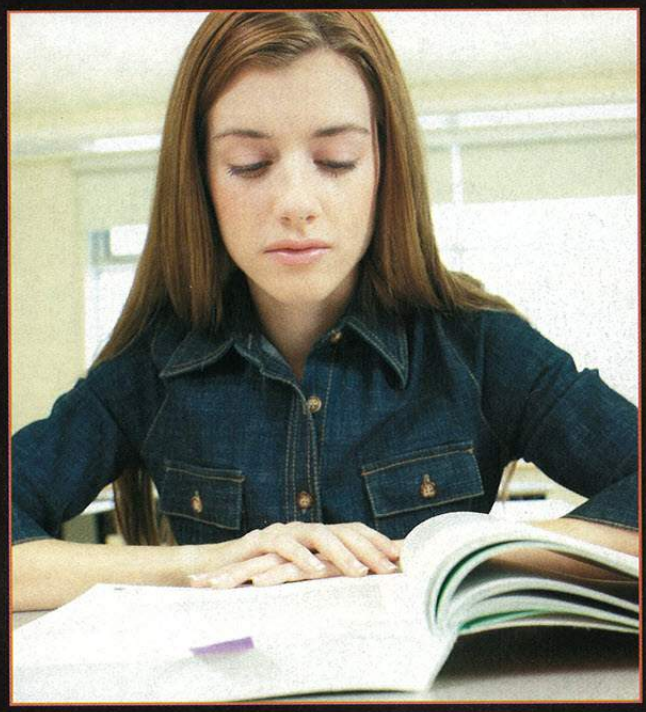
Une oreillette, voilà l'arme possible pour l'examen de langue. Elles sont tellement petites que l'on y voit "presque" que du feu. Si le professeur demande ce que c'est, le "Je suis malentendant" peut-être une solution. Un cas a même été détecté au moment où l'élève sortait un document médical prouvant son problème de surdité. Vendu entre : 80 euros et très cher.
http://www.alifax.fr/recherche.asp

EXAMEN MATHÉMATIQUE

Aujourd'hui les calculatrices ressemblent de plus en plus à de petits ordinateurs de poche et certains PDA ont de quoi faire rougir certains ordinateurs. Comptez entre 200 et 1 000 euros selon le monstre de course que vous souhaitez.
http://www.bargainpda.com/

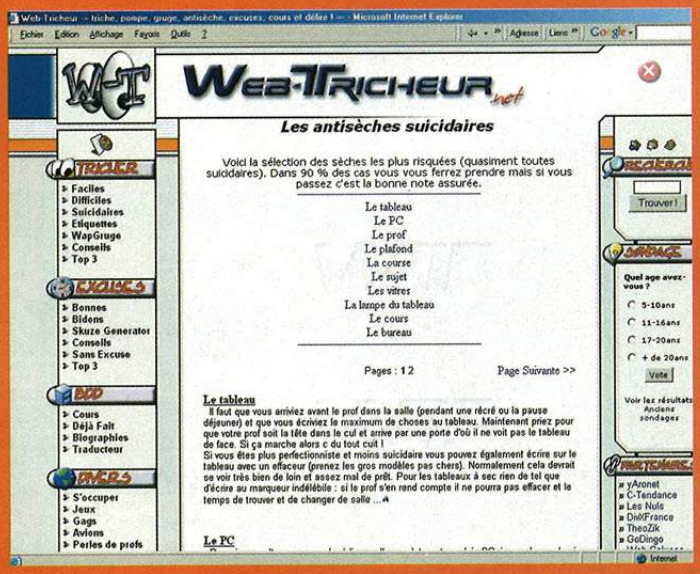
LE BON, LA BRUTE ET LES TRUANDS.

Les cas de tricherie par l'informatique sont devenus de plus en plus courants depuis quelques mois. En voici quelques-uns. Six étudiants de l'école de Fremont de San José, en Californie, ont été suspendus le 6 mars dernier après la découverte du piratage des ordinateurs de l'école. Les six élèves s'étaient introduits dans la machine de gestion des bulletins de notes afin d'y modifier leurs classements. Les 6 "tricheurs" ont été épinglés après que leur professeur principal ait découvert qu'ils avaient eu les réponses via SMS. Des comparses à l'extérieur de la salle, connectés à Internet, envoyaient les réponses. Les loulous avaient scotché les GSM sous les bureaux.
Une étudiante de l'université de Delaware (USA) a été arrêtée pour avoir piraté les comptes informatiques de ses professeurs pour y modifier ses notes. Pas bonne en mathématique, en science et social, Darielle, âgée de 22 ans, a transformé ses F en A. En gros elle a passé ses notes de 5 à 20, discret !
Elle a été libérée après avoir payé une caution de 5.500 dollars. Ca fait cher le bonnet d'âne.
On ne pouvait pas finir notre série d'exemples sans le cas de Reid Ellison, un étudiant de haut vol de la Anzar High School basée à San Juan Bautista. Il a décidé que l'un de ses dossiers d'examens porterait sur le hacking. Il a demandé l'accord de ses professeurs, qu'il a eu. Très bon élève, il a voulu montrer que modifier les notes n'était pas si compliqué. N'ayant que des A, il a donc baissé sa propre moyenne. Fayot !



LE WEB TRICHEUR

« Après des années d'investissements, de recherche et d'expérimentation mais aussi l'aide d'innombrables ingénieurs, bricoleurs et cobayes nous avons réuni pour vous un concentré d'informations concernant la triche au lycée, à la fac, au collège, en primaire et même parfois la maternelle ! » Voilà comment commence le site de Web-Tricheur. Marrant, parfois efficace, il propose toutes les astuces pour tricher. Bonus, une option pour fabriquer son antisèche pour son téléphone wap.
http://www.web-tricheur.net



BOSSER, LE MIEUX DE TOUT

Si vous êtes plutôt du genre à bosser, ce qui est plutôt la meilleure des solutions, deux sites incontournables regroupent à eux deux : fiches de lectures, mémoires, informations sur les examens, les méthodes de révisions…
http://www.oboulo.com et http://www.bibelec.com. Il faut savoir pour finir, que la tricherie peut vous coûter cher. En France tricher lors d'un concours officiel est un motif d'élimination avec interdiction de repasser un examen dans les 5 années suivantes.

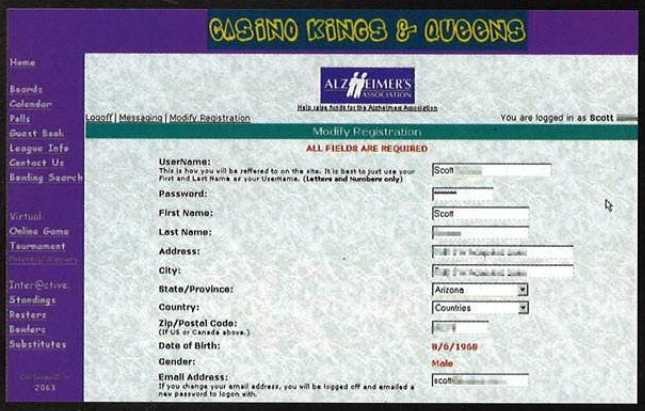
LES PIRATES NE SONT PAS MANCHOTS

Les casinos en ligne pullulent sur le web. Promesse d'argent facile, de frisson face aux roulettes virtuelles et possibilité de blanchiment d'argent rapide dans certains cas. Les casinos online sont aussi la cible des pirates et aussi étrange que cela puisse paraître, certains casinos se fichent comme de leur dernier BlackJack de la sécurité de leurs services. Une enquête exclusive de Zataz Magazine.

MONEY, MONEY, MONEY

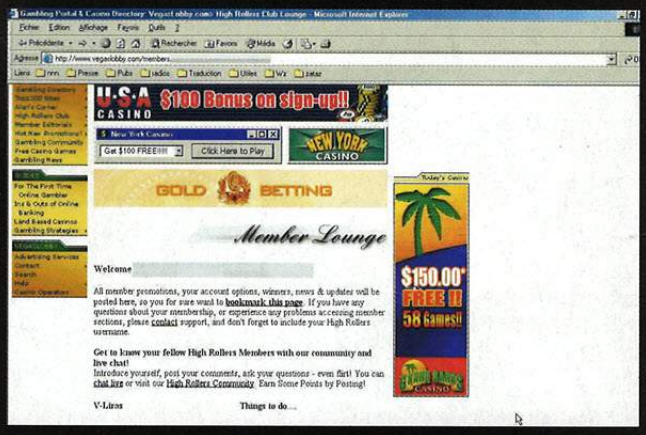
Des casinos online il y en a partout. Les publicités, illégales en France, tombent comme neige au soleil sur les sites web, dans les mels, les popups... Promesse du moment, gagner de l'argent facilement. Les casinos annoncent quasiment tous une redistribution de 95 % des gains joués. Une manne financière qui ne pouvait pas laisser indifférents les escrocs numériques et les pirates. Nous avons voulu savoir si les casinos étaient protégés. Normalement oui, dès que l'on parle d'argent sur le web, les administrateurs regardent de plus près à ne pas voir leurs clients, et eux même, se faire piller.
On va malheureusement vous décevoir. Nous avons découvert plus de 80 casinos Internet ouverts à tous les vents.

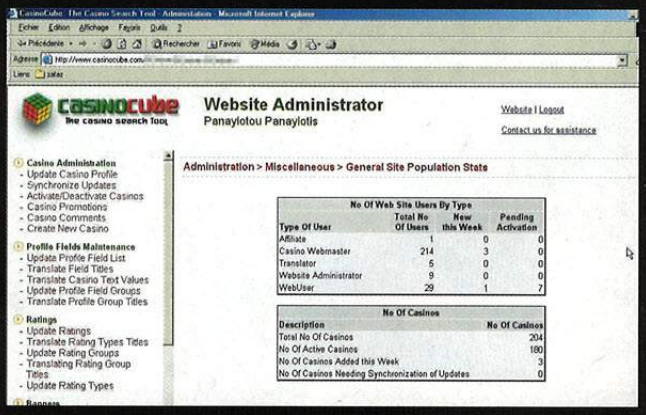
CACHEZ DONC CE JACKPOT QUE JE NE SAURAI VOIR

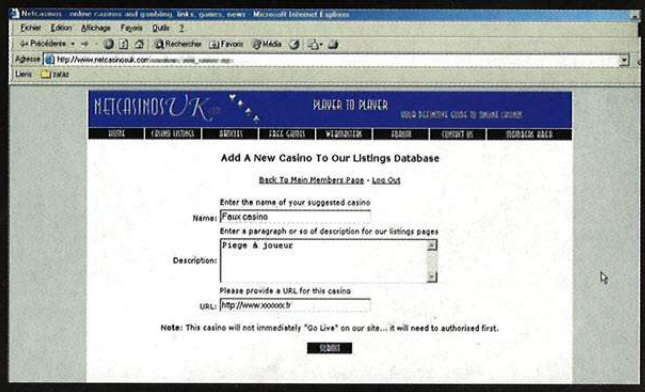


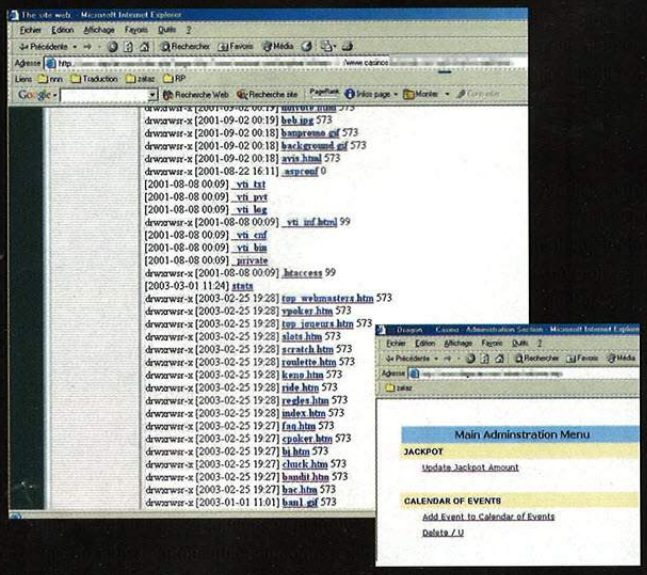
Notre technique n'a pas été des plus révolutionnaires, mais semble être malheureusement très efficace. Pardon de frustrer les plus avides d'entre vous, mais pas question pour nous de vous expliquer comment accéder à ce que nous allons vous montrer. Notre but est de vous alerter du danger et pas de vous transformer en cyber-criminels. On doute que passer les prochains mois en prison puisse vous intéresser ! Premier de nos exemples, les casinos qui ne protègent pas du tout leurs clients. Nos premières photographies montrent comment il était possible de prendre l'identité d'un joueur, donc de modifier les informations pour recevoir leurs gains... ou pire, les ruiner d'un coup de dé numérique. Faille découverte dans une quarantaine de casinos online.

Autre exemple, la modification des informations mises en ligne sur le site du casino, nous avons découvert une trentaine de casinos faillibles à ce genre de problème. Imaginez mettre un faux site, et voir vos sous disparaître dans les poches d'un escroc. On ne parle pas de la possibilité de mettre un trojan, un espion numérique, dans l'un des jeux à télécharger.









Nous terminerons avec deux exemples ultimes. Le premier, la possibilité de "gagner" et/ou de modifier les jackpots. Imaginez le problème pour le casino. Vous modifier les informations du jackpot, de manière à gagner, par exemple, 10.000 fois la mise, au lieu des 100 promis. Nous avons découvert 4 sites offrant cette terrible option. Le dernier cas, imparable, est la possibilité de rentrer dans le serveur via une faille ou tout bêtement un backdoor. Nous avons découvert un seul casino faillible à ce problème mais ici tout était possible.

DES CHIFFRES ET DES LETTRES

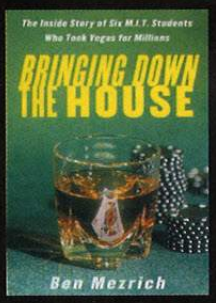
Le piratage de casino ne se passe pas que sur le web. Nous avons rencontré Benoît, un informaticien britannique, qui travaille pour une chaîne de casinos de sa gracieuse majesté. L'anonymat étant de mise, il a bien voulu nous parler sans citer son entreprise qui a vécu un étrange cas au mois de février dernier. "Un joueur a gagné 300.000 Livres Sterling via 4 machines et cela en moins de 2 heures (...) Nous sommes toujours en train de chercher comment il a pu faire (...) il a été payé mais aujourd'hui il est sur une blacklist qui lui interdit l'accès aux casinos du pays".

Comment est-ce possible, notre interlocuteur n'en sait rien, ou du moins n'a pas souhaité nous le dire. Les cas de piratages d'un Jackpot ne sont pas courants, il faut dire aussi que le secret professionnel oblige les salariés à un bouche cousue de rigueur. L'un des derniers cas connus date du mois de mars dernier. Un pirate canadien avait découvert comment piéger certaines machines à sous de la marque VLT. Un problème qui a obligé l'Atlantic Lottery Corp à remplacer les puces informatiques dans plus d'un tiers de ses 3 538 machines. Environ 20 emplacements avaient été utilisés par le pirate et ses complices. ALC ne sait pas combien d'argent il a pu perdre et n'a pas souhaité communiquer sur le procédé du pirate... loin d'être manchot.

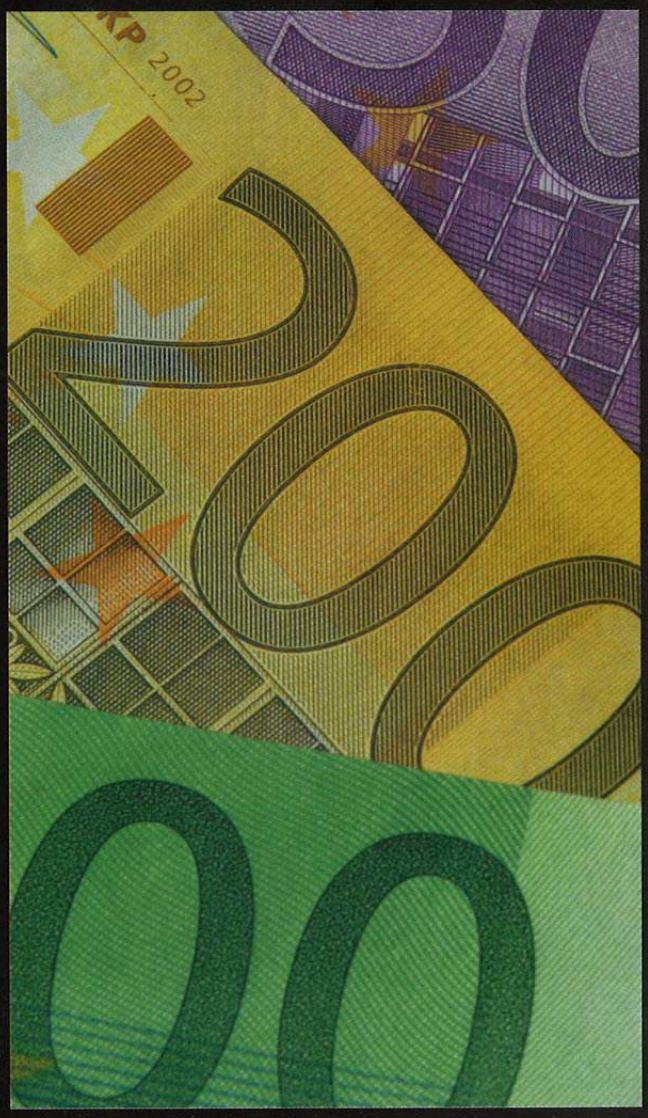
CASINO ET MAFIA

Nous avons posé la question à plusieurs casinos online sur le sujet Mafia et machine à sous virtuelle. "Il ne faut pas pousser ! Parler de mafia, fraude on-line et casinos on-line, sont bien trois choses distinctes, même si il peut arriver que les uns utilisent les autres.". Il est vrai que plusieurs banques ont mis en garde leurs clients au sujet des casinos. Les cartes (MasterCard, Visa, etc.) n'aiment pas les casinos en ligne parce qu'il y a beaucoup de répudiation. Le joueur qui perd, aura très facilement tendance à dire que ce n'est pas lui qui a misé. Détail important les casinos sérieux arrivent quand même à maintenir ce taux largement en dessous de 1%. Les banques elles-mêmes ont reconnu que 80% des numéros de cartes volés l'étaient via les "facturettes" émises par les machines des commerçants ou les distributeurs de billets, et non pas directement via Internet. "Si un mafieux veut blanchir de l'argent avec un casino en ligne, la méthode est la même qu'avec un casino "réel" : être propriétaire, et y faire perdre ses hommes de main. Résultat : le casino a fait des gains parfaitement légaux en apparence, et son propriétaire peut en disposer sans être inquiété légalement !" dixit notre contact. La plus grosse fraude sur les casinos en ligne est de tout simplement "plumer" le joueur en ne versant jamais de jackpot ou autre gain autre que tout petit pour appâter les gogos.

MIT BLACK JACK TEAM



On se devait de finir cet article par l'histoire folle de 6 étudiants du MIT, le Massachusetts Institut technology. Ce nid à matheux a été le terrain d'une expérience folle. 1993, un professeur de cette prestigieuse université de Boston a entraîné ses élèves à tricher au casino. Comment ? Par le calcul mental. Le plus fou est qu'ils vont réussir à gagner entre 1 et 5 millions de dollars directement via les tables BlackJack des casinos de Las Vegas. Il faut savoir qu'à la différence des autres jeux des casinos, le BlackJack possède une mémoire. L'idée est d'atteindre le score de 21 points pour gagner à tous les coups. Les 6 étudiants vont trouver une méthode qui leur a permis de connaître les cartes contenues dans les 6 paquets de 52 cartes. Une arnaque de première car chaque étudiant ayant son rôle propre. Celui qui compte, celui qui joue au flambeur pour détourner l'attention, celui qui montre qu'il compte et se plante... Bilan, 154 % de retour sur investissement. A noter que l'acteur Kevin Spacey tourne en ce moment un film tiré de l'histoire de ces escrocs de génie. Le film est tiré du livre du même nom : Bringing down the house. La sortie en salle est prévue fin 2003.

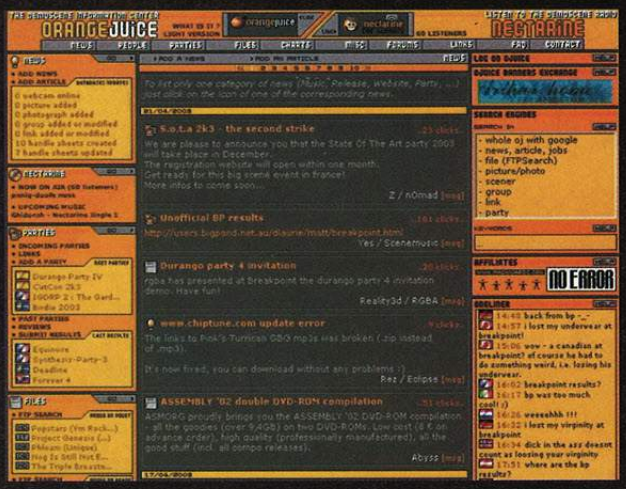


DEMO'NIAK

Comme chaque mois nous allons faire un petit tour du côté des créatifs de l'underground informatique, les démomakers. Attention, ça va être hot !

OJUICE

Voici le site à bookmarker en quatrième vitesse. Informations sur les party, les groupes du moment. Des interviews et des productions à télécharger. Le must dans son genre. Seule ombre au tableau, la langue de Shakespeare obligatoire.
http://www.ojuice.org



TÉLÉCHARGEMENT

Le site scène.org est le centre de stockage qu'il vous faut garder sous la souris en cas de besoin de production, vieille ou non. Vous avez un nom de démo en tête, vous cherchez, vous aller trouver.
http://www.scene.org/news.php

QUAND LA MUSIQUE EST BONNE

Le site de la scène musicale underground. Les amateurs de samples, chips song, compositions, vont pouvoir s'en exploser les oreilles.
http://noerror.scene.org/

CONSOLES

Pour les amateurs de démos dédiées aux consoles de jeux on ne peut que vous conseiller le site japonais kmkz. Petit frein cependant pour s'y retrouver, savoir causer le nippon.
http://kmkz.jp/mtm/

CAMARADES

La Russie est connue pour la qualité de ses informaticiens. La scène démomakers n'y est pas nouvelle là bas, pour preuve, le site Démo Scène russia qui propose les créations des codeurs du cru.
http://www.demoscene.ru/english/news/

PAPY FAIT DE LA RESISTANCE

La scène démo sur Amstrad CPC n'est pas morte. Il existe toujours des férus de cette machine 8 bits. Certaines démos sont d'ailleurs à couper le souffle quand on connaît cette machine.
http://cpcscene.dyndns.org/

A NOTER DANS VOS AGENDAS

IGDRP 2 : The Garden Dwarf Strikes Back
09 au 11 mai à Villers les Nancy.
http://igdrp2.fr.fm/

AMSTRAD CPC Expo 2003
07, 08 et 09 Juin Espace Jeunes (F.J.T.) à Coutances (50)
http://www.manchoo.com/expo

ASSEMBLY '03
L'incontournable Assembly. L'une des plus importantes démo party de la planète.
Elle va se tenir du 07 au 10 août 2003 à Helsinki, en Finlande.

SOTA 2003

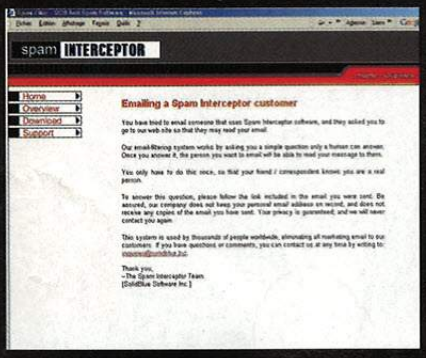
Nous vous parlions dans ZATAZ Magazine numéro 6 de la State of the art party. Et bien souriez, elle revient en décembre prochain dans le nord de la France, du côté de Lille.
http://www.stateoftheart.fr.st/

Les Party VIP et Slasch sont annulées pour cette année en France. À suivre !

BONS PLANS

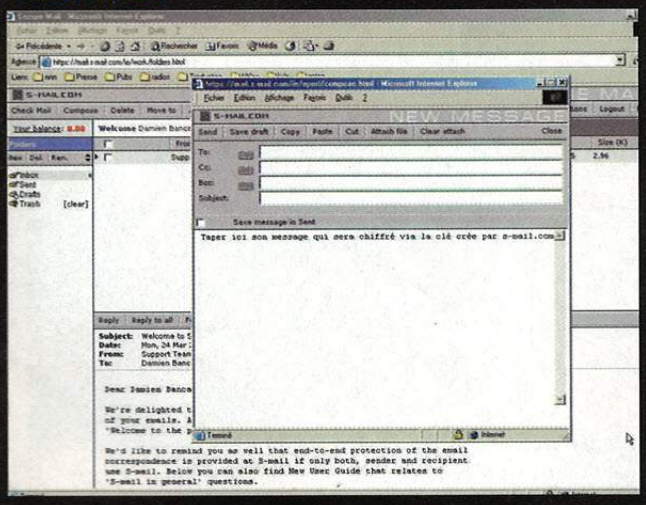
Il existe sur le réseau des réseaux une pléthore de logiciels permettant de sécuriser nos surfs. Voici notre meilleure sélection du moment, avec, cerise sur le gâteau, deux logiciels 100 % ZATAZ Magazine rien que pour vous.

ANTI-SPAM



Le site Spam Interceptor va vous permettre de protéger vos mels des tonnes de publicités non sollicitées. Simple de fonctionnement, vous rentrez vos coordonnées d'émission/réception, Spam Interceptor fera le reste. Dès qu'il considère qu'un mel est litigieux, il renvoi un courrier à l'émetteur du spam possible. Il faut cliquer sur un lien, rentrer un code qui s'affiche à l'écran pour s'assurer que le mel envoyé ne l'a pas été fait pas un robot. Efficace ! http://www.si20.com/explanation.php
Voir aussi : http://www.mailcleaner.net/

MELS CODÉS



Il existe énormément de système et logiciels qui permettent de chiffrer nos mels. Malgré les propositions de transformer le chiffrement en arme à terroriste, il est intéressant de voir qu'aux USA les services qui permettent de protéger la vie privée ne disparaissent pas. Dernier en date, S-Mail, un webmail permettant de chiffrer et protéger les envois de ses mels grâce à SSL et OpenPGP intégré. Le système est gratuit. Interressant si on ne transporte pas avec soit son GPG et ses clés de chiffrement. http://www.s-mail.com

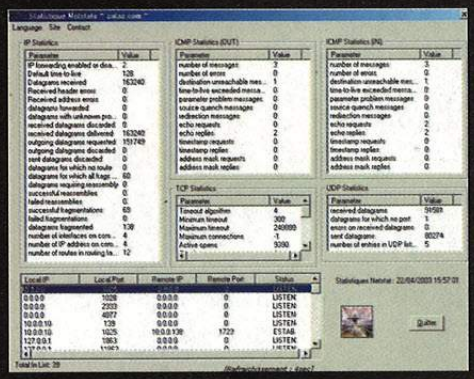
ANTIVIRUS GRATUITS ONLINE

Vous avez été nombreux à nous poser la question à savoir s'il existait des antivirus gratuits directement consultables sur le réseau des réseaux. Nous vous conseillons de tester celui de Panda Software, notre préféré, ainsi que celui de Trend Micro. Le fonctionnement est simple. Un petit module se télécharge sur votre machine, il ne reste plus qu'à scanner votre PC à la recherche d'une bestiole numérique. http://www.pandasoftware.com/activescan/fr/activescan_principal.htm
http://fr.trendmicro-europe.com/index_personal.php
http://www.ravantivirus.com/scan

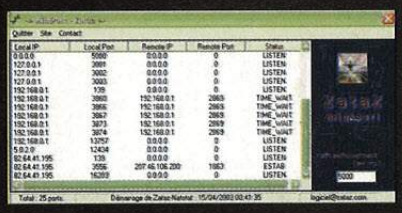
CHAT CODÉ

Nous vous en avions parlé en avant-première voilà un an. La société française Secway vient de sortir sa nouvelle monture de SIMP, traduisez par Secway's Instant Messenger Privacy. SIMP va chiffrer vos messages de manière efficace et facile sous MSN, Yahoo, ICQ, AOL... Une clé de chiffrement va être crée et diffusée à vos correspondants. Elle vous permettra de chiffrer à la volée vos informations sans crainte de lecture par une tierce personne. Une version commerciale est sortie au mois d'avril au prix de 25 euros/dollars.
http://www.secway.com

NETSTAT



Vous avez toujours voulu savoir ce qui se tramait pendant vos surfs. Quels logiciels ouvraient quels ports de votre ordinateur ? Notre programme Netstat va tout vous dire : qui, quoi, comment, où, quelle adresse IP.



Bref de quoi contrôler le flux d'information rentrant et sortant de votre machine connectée sur Internet. Nous avons réalisé plusieurs versions, light ou plus poussées pour que chaque utilisateur y trouve son compte.
http://www.zataz.com/zatazv7/logiciels.htm

LE PASS'FLIPZ'TAZ

Qui n'a jamais flanché face à son mot de passe ? Qui n'a jamais calé devant la création d'un mot de passe ? Qui n'a jamais voulu balancer loin, très loin, son ordinateur car vous aviez oublié le mot de passe du document Word que vous aviez mis en place. Bref, voilà l'outil qu'il vous faut. Fabrication 100 % ZATAZ Magazine, il va vous permettre de retrouver tous les mots de passe de votre machine, de décoder ceux cachés par des étoiles, de générer autant de mots de passe que vous en aurez besoin et cerise sur le gâteau, la version 2, comportera un "brute force" qui vous permettra de casser votre document Word, zip que vous avez protégé par mot de passe sans penser à noter ce dernier.
http://www.zataz.com/zatazv7/logiciels.htm

SERVEUR TROUÉ, SORTEZ LES RUSTINES

Comment repérer les failles dans votre serveur ? Comment les corriger et donc vous protéger ? Voici un petit tour d'horizon des failles les plus utilisées par les pirates.

BÉA-BA !

Tout d'abord, il n'y a pas de secret, il vous faut être un administrateur attentionné et rigoureux. Les mises à jour arrivent presque chaque mois et les services que comportent votre serveur doivent être mis au goût du jour sous peine de le voir se transformer au goût des pirates. Nous allons donc vous énumérer les différents exemples de failles ainsi que le patch à mettre en action. Attention, sachez que ceci n'est que la face visible de l'iceberg, donc pensez à faire appel à de vrais professionnels de la sécurité informatique.

LE SYSTÈME WINDOWS

Soyez rigoureux en particulier avec Windows. Il comporte pas mal de failles et son utilisation par 95 % des ordinateurs de la planète le transforme en un terrain de jeu propice aux pirates.

LA FAILLE UNICODE

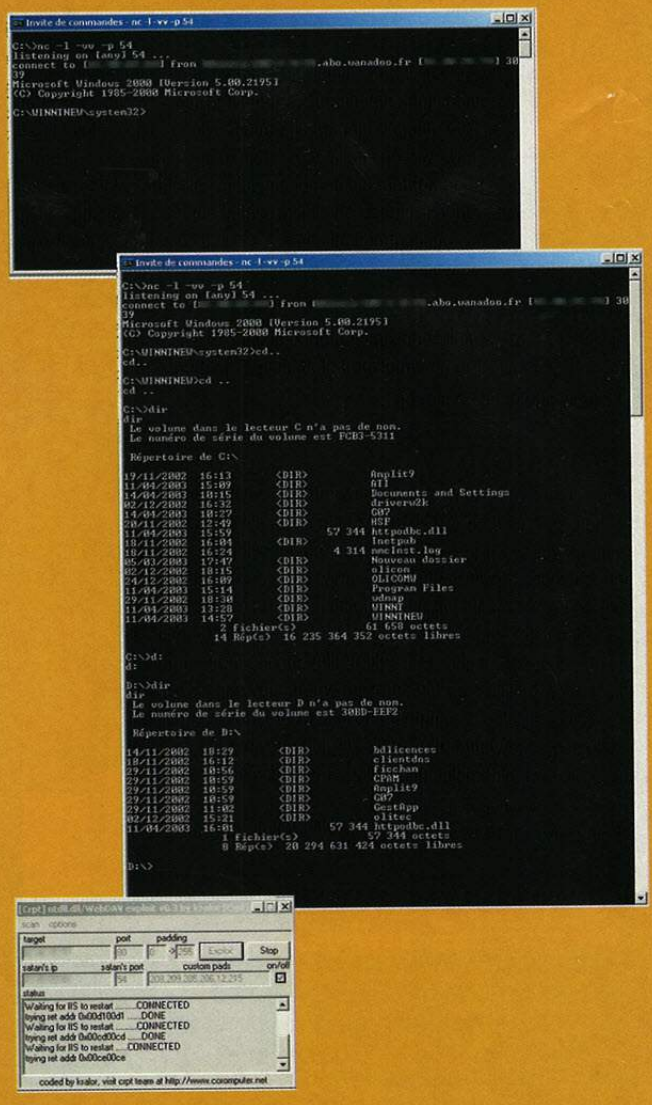
Apparu en 2001, ce bug agit sur les serveurs IIS. Lorsque vous envoyé une requête de type : " /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\ " le serveur IIS va mal traduire les caractères unicodes présents dans la requête. Bilan, cela va donner aux pirates l'accès au serveur avec la possibilité d'utiliser le cmd.exe pour l'explorer. Il faut savoir qu'il y a différentes requêtes concernant la faille unicode. Elles diffèrent selon le pays hébergeant la machine. Beaucoup de serveurs demeurent encore vulnérables. Si c'est votre cas, utilisez notre logiciel ZUNICOZ, que vous trouverez dans notre rubrique Logiciels pour vous en assurer. Si, lors de l'exécution de notre programme vous apercevez le listing de votre disque dur c:\ , alors votre server est vulnérable. En conséquence vous devez télécharger le patch disponible à l'adresse suivante :
http://www.microsoft.com/ technet/security/bulletin/MS01-027.asp

LA FAILLE D'EXTENSION FRONTPAGE

Cette faille concerne le partage de dossiers avec le logiciel Frontpage. Un internaute peut facilement lister et modifier les données du site, mais il peut aussi télécharger, sur le serveur ciblé, un fichier en php qui va lui permettre de lister le server entier. Un backdoor comme nous vous l'expliquions dans ZATAZ Magazine n'6. Plusieurs solutions à ce problème existent: modifier les permissions concernant les utilisateurs et les groupes, le mieux étant bien sûr de téléchargez le patch qui corrige cette faille :
http://download.microsoft.com/download/win2000pro/Patch/Q324096/NT5/FR/Q324096_W2K_SP4_X86_FR.exe

LA FAILLE WEBDAV

La faille WEBDAV a fait pas mal parler d'elle en mars et avril dernier. Les pirates l'ont utilisée pour frapper d'importants sites, comme des gouvernements. Elle tourne sur des serveurs IIS 5.0 sous Windows 2000. Une vulnérabilité critique dans un composant de Windows 2000 utilisée par le protocole WebDAV (World Wide Web Distributed Authoring and Versioning) peut permettre à une personne malveillante de planter ou d'exécuter le code de son choix sur un serveur IIS 5.0 utilisant ce système d'exploitation, en envoyant une requête HTTP spécifiquement malformée. Cette faille est spécifique à Windows 2000 et ne concerne pas IIS 5.0 sous NT 4.0 ou XP.



Pour exploiter cette faille, les pirates ont plusieurs possibilités. Beaucoup utilisent "superscan" qui permet de scanner la machine cible sur le port 80. Cela permet aux pirates d'avoir le type de serveur présent. Ils n'ont plus qu'à démarrer netcat sur le port 54 et utiliser l'exploit ntdll.dll/WEBDAV créé par un hacker nommé Kralor, sur le port 54.

Si la faille est présente, le pirate aura un accès administrateur sur le serveur cible. Il va pouvoir ensuite se balader sur les différents disques durs de sa cible, y copier des fichiers, en télécharger, ou modifier... Cette faille exerce un débordement de tampon sur le fichier ntdll.dll et permet avec un offset précis de donner l'accès. Le patch se trouve sur le lien suivant :
http://www.microsoft.com/security/security_bulletins/ms03-007.asp

Le groupe Coromputer, fondé en 1998, a été le premier à sortir un exploit pour Webdav. Le programme qui en découle permet de prendre la main sur un serveur Windows 2000 faillible. Nous avons rencontré "l'inventeur", Iván Rodríguez Almuiña aka, Kralor un chasseur de bits pas comme les autres.

Comment vous est venue l'idée de cet exploit ?
Ca faisait des mois que nous n'étions plus que Spyd et moi sur IRC à raconter des conneries et l'advisory sur ntdll.dll through webdav est sorti. J'ai tout de suite sauté sur l'occasion. Je venais de finir quelques shellcodes hardcoded offsets free, utilisant les techniques de SEH+ScanMem et PEB [private] dont le reverse remote shell que j'ai utilisé pour coder l'exploit Webdav. J'ai alors réalisé l'exploit et là tout a commencé à bouger, à un point que cela m'a donné mal à la tête à force de lancer ma boite de courriers électroniques.

Votre "découverte" a été volée, cela ne vous gêne pas ?
Oui ça me gène. Imaginez, passer des journées de 16h, deux nuits blanches afin de réussir à trouver un bon moyen pour coder l'exploit. Je le code et un gars que je ne connaissais pas du tout, RaFa, le prend, rajoute son mel et poste mon exploit sur la mailing list de sécurité informatique la plus connue, celle de Security focus. Bien évidemment beaucoup de gens ont cru que c'était lui Kralor à un point tel que j'ai même reçu une proposition d'emploi qui a était envoyée sur mon e-mail ainsi que sur le mel de Rafael Nunez, le voleur en question.

Et depuis ?
Depuis le premier e-mail je n'ai plus jamais eu de nouvelle. J'en déduis donc qu'il m'a piqué le boulot. C'est dans ces cas là que je suis énervé. Rester dans l'obscurité ne me gêne pas, mais là ...

Est-ce cela l'ambiance de la communauté underground, se faire voler ses découvertes ?
Alors pour que cela soit bien clair Rafael Nunez n'a rien à voir avec la communauté underground. C'est un pseudo professionnel de la sécurité, c'est d'ailleurs comme cela qu'il se décrit. Tous les " hackers " que je connais ont valeur du respect. On s'échange des infos, on apprend sans cesse mais il y a un acte qu'on ne pourra jamais faire, voler une découverte ou une technique. Sans morale on ne va nul part. Dans tous les cas je ne fréquente jamais ce genre de " gars " capables de s'approprier une découverte.

Diffuser une info comme Webdav et la voir utilisée par des pirates ne vous gene pas ?
Personnellement je ne vois pas pourquoi je serais gêné. C'est plutôt les administrateurs des serveurs qui se font pirater... et Microsoft qui devraient être gênés.

LE SYSTÈME SUNOS/SOLARIS

Les systèmes SunOS/Solaris contiennent une faille principale qui est la plus utilisée par les pirates. Il en existe. La faille concerne les systèmes SunOS/Solaris 5.x ayant le port TELNET, le port 23 ouvert. Par conséquent le Telnetd est activé sur le serveur. Le principe de la faille est "habituel", un Buffer overflow, comprenez un débordement de tampon, est exercé sur le Telnetd donnant l'accès root à l'utilisateur malveillant.
Il permet aux pirates de devenir administrateur et donc d'agir à sa guise.
Le patch pour ce buffer overflow : http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F28063

LE SYSTÈME LINUX

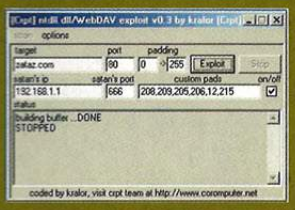
Le système linux peut contenir diverses failles, cela dépend de la configuration de celui-ci. Il peut avoir une faille sur le port SSH, le port 22, si vous avez configuré votre server avec le SSHd. Si vous rajoutez une version OpenSSh pas très récente, votre système devient vulnérable. Comme d'habitude, les failles se ressemblent à peu près toutes : que ça soit sur le port Telnet, SSH, ou autres, cela apparaît principalement via un buffer overflow.

Un exemple : Le service OpenSSL. L'utilisateur peut avoir accès au serveur avec les permissions d'un utilisateur lambda. Il peut utiliser un "local exploit" qui va lui permettre de lui donner les droits de l'administrateur. L'exploit d'OpenSSL se base sur la connexion aux ports OpenSSL, les ports 443 et 444. Ici encore un buffer overflow va être utilisé sur un offset précis suivant la version du Kernel et de son type. Il est très important de faire des mises à jours de vos versions d'Apache, d'openSSL, de mod_SSL ... mais aussi de votre Kernel. Amateurs de compilation à vos souris.
Pour patcher votre OpenSSL sur une distribution Redhat 7.1 avec un processeur i386 par exemple, il vous faudra agir ainsi :
wget ftp://updates.redhat.com/7.1/en/os/i386/openssl*
rpm -Fhv openssl*

Pour d'autres distributions nous vous conseillons de vous rendre sur le site www.rpmfind.net

Nous ne parlerons pas ici d'OpenBSD et Freebsd. Ils ont un point commun avec Linux, leur base Unix. En conséquence même s'ils sont différents, nous vous conseillons de suivre les mêmes conseils que pour Linux. Mais n'oubliez pas que ceci n'est qu'une poignée de sable dans un désert, la sécurité de vos serveurs doit se coupler avec des gens compétents et une veille régulière.

AUTOMATISATION DE WEBDAV

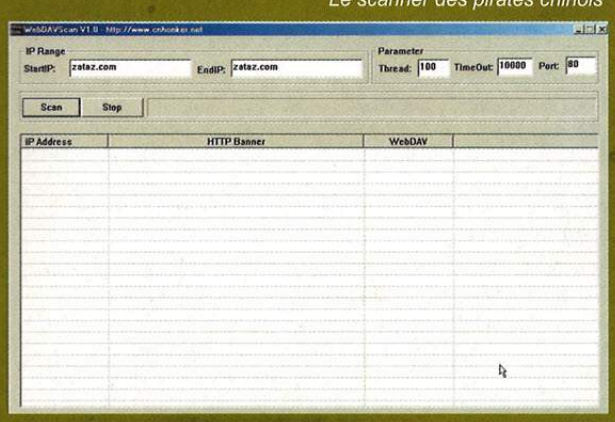


L'outil de kralor

A chaque grosse faille, certains hackers mettent en place un exploit, un procédé qui va permettre l'utilisation de cette faille. Dans le pire des cas, des logiciels automatisent la procédure, ouvrant la porte aux pirates et autres script-kiddies. La faille Webdav n'a pas dérogé à la règle.

Le premier programme, crée par Kralor (Voir son interview, ndlr), pèse à peine 52 kilos. Il permet de trouver et permettre l'exploitation de Webdav. "Le fait qu'on se soit fait spolier notre découverte par Rafa et des journalistes peu scrupuleux de connaître la vérité avant de sortir un article, inconsciemment ca nous a donné l'envie de nous venger et de sortir des programmes encore plus Féroces " Dixit l'auteur de cet exploit de la team Coromputer.
Un autre programme encore plus dangereux a vu aussi le jour sous le nom de KaHT. Le pirate, aT4r@3, propose un programme sous dos qui a la particularité de scanner plusieurs ip en même temps, de générer un rapport en html des ip piratables, il permet aussi d'uploader des scripts, de brute forcer et de créer des comptes admins. Bref, un couteau "suisse" du pirate qui risque de faire pas mal de dégâts. Pour finir dans la série des outils dangereux, les chinois du CNhonker, nous vous parlions d'eux en janvier dernier avec le virus SQL, ont sorti un scanner Webdav. Il scanne des ranges d'ip afin de récolter les bannières http afin de trouver des serveurs IIS 5.0 et testé la faille Webdav sur ces derniers. Bref, des outils qui n'ont pas intérêt a à tomber entre de mauvaises mains.

Le scanner des pirates chinois



UTILISER LINUX SANS L'INSTALLER

Avec le nombre impressionnant de versions différentes de Linux disponible en téléchargement sur le réseau, difficile de faire son choix. Des internautes français de la Fédération Informatique et Libertés ont sorti celui qu'il vous faut. Une version de Linux prête-à-l'emploi et supportant le chiffrement fort : "Knoppix-Mib".

LINUX-KNOPPIX, KESAKO

Le CD-ROM Knoppix-Mib a été développé par Michel Bouissou, membre fondateur de la FIL, programmeur Linux, on lui doit par exemple un système de chiffrement de disque dur. Basée sur Linux-Knoppix, une version conviviale et grand public du logiciel libre Linux, "Knoppix-Mib" ne nécessite pas d'installation et s'exécute depuis le CD-ROM sans rien inscrire sur le disque dur de l'ordinateur. Il s'agit d'un CD-ROM conçu pour être utilisé en déplacement, mais aussi chez soi. Chose particulièrement intéressante, 95% des matériels sont détectés automatiquement sans nécessiter d'installation particulière de plugin. Le CD-Rom étant bootable, pas besoin de l'installer sur la machine. Même si cette option est possible. Linux-Knoppix s'exécute entièrement dans la mémoire virtuelle de votre PC, le CD ne modifiera rien sur vos disques durs à moins que vous ne lui demandiez, et ne détruira donc pas les autres systèmes d'exploitation que vous avez pu installer.

SÉCURITÉ BIEN ORDONNÉE

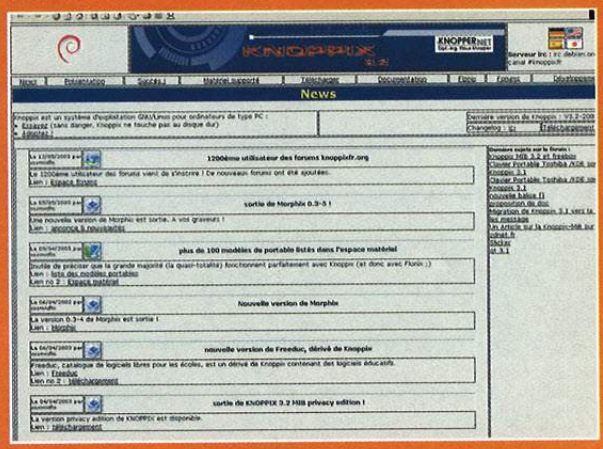
Linux-Knoppix permet, pour plus de confidentialité, de chiffrer la mémoire virtuelle, la swap, de votre ordinateur ainsi que les répertoires /home des utilisateurs/trices, qu'ils soient sur le disque dur ou non, avec la possibilité d'héberger ces fichiers sur des périphériques externes comme une clef mémoire USB ou une disquette ZIP. Impossible donc d'accéder à vos fichiers sans connaître votre mot de passe. Si vous êtes nomades, ou utilisez des ordinateurs qui ne sont pas les vôtres, il vous suffit donc d'avoir le CD de Knoppix sur vous et votre périphérique externe contenant votre répertoire personnel pour accéder à vos fichiers en toute confidentialité et en ne laissant aucune trace sur ces ordinateurs. Si vous perdez le périphérique de stockage contenant vos fichiers personnels, la personne qui le trouvera ne pourra pas lire vos fichiers puisqu'ils sont verrouillés par cryptage.

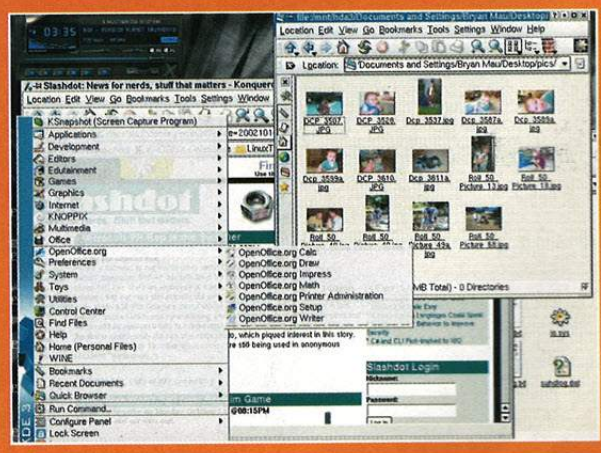
ET LE MATOS ?

Linux-Knoppix dispose en outre d'une panoplie de programmes en faisant un système complet, capable de lire tous types de fichiers multimédia avec XMMS, de documents textes (propriétaires ou non) grâce à OpenOffice 1.2.2, de naviguer sur internet avec Konqueror ou encore Mozilla, de gérer ses e-mails via un serveur Postfix qui permet d'éviter de passer par votre fournisseur d'accès et des outils comme Kmail ou encore Ximian Evolution, de vérifier la sécurité de votre réseaux en codant par exemple vos messages via le logiciel GnuPG, le PGP libre, de dessiner grâce à The Gimp, de graver vos CD-ROM avec le logiciel K3B, ... Bref, vous recherchiez un Linux, souple, facile d'accès et sécurisé {?} Il ne vous reste plus qu'à graver l'ISO que vous pouvez télécharger gratuitement via zataz.com.

LIENS UTILES

http://download.vie-privee.org/
ftp://download.vie-privee.org/lafil/
ftp://ftp.vie-privee.org/lafil/
ftp://ftp.apinc.org/lafil/
ftp://ftp2.ael.be/mirrors/ftp.vie-privee.org/lafil/





PS2™

XBOX

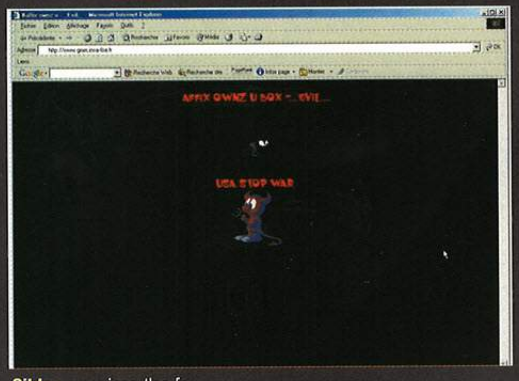
LES SITES PIRATÉS DU MOIS

Il s'en passe de drôle sur le réseau des réseaux. Voici otre sélection des sites Internet piratés soit par des scripts kiddies en mal de reconnaissance, soit par des hacktivistes ayant trouvé ce moyen pour faire passer leurs messages. Cette page est en collaboration avec notre partenaire Force-h. Si vous aussi vous êtes témoin d'un piratage de site web, contactez-nous via contact@zataz.com.

Cible : Aquastream.fr
Auteur : Diabolax
Commentaire : Depuis la guerre en Irak ce site a vécu plusieurs modifications donc celle de Diabolax. Ce dernier avait souhaité faire passer son propre message sur la politique de George W. Bush. D'après ce pirate, " Bush is Monky ".

Cible : La voix des opprimés
Auteur : Ironic Boy
Commentaire : Ce groupe brésilien s'est attaqué à un site pro palestinien. Pas de message politique, juste un superbe dessin qui a dû prendre 100 fois plus de temps que le piratage en question.

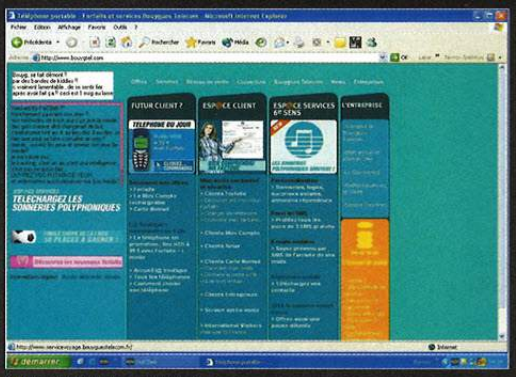
Cible : Men of God
Auteur : Heart of David
Commentaire : Le site des fans des mercenaires américains quelque peu malmené par ce groupe d'hacktiviste français. Le " HoD " va faire le pied de nez aux soldats de fortune de l'Oncle Sam.



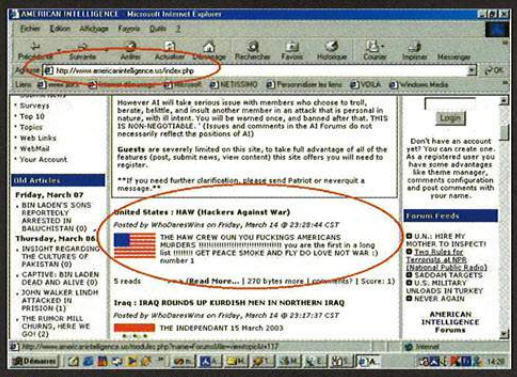
Cible : gmm.insa-tlse.fr
Auteur : Evil
Commentaire : L'Institut National des sciences appliquées de Toulouse visité par un diablotin. Rien de révolutionnaire juste un besoin de laisser sa trace. Passe le concours petit diable, après on verra pour ton admission dans cette école.

Cible : CCI du Morbihan
Auteur : Kernel Panic
Commentaire : La Chambre de Commerce et de l'Industrie du Morbihan modifié par le groupe brésilien, et oui encore, Kernel Panic. Ces kiddies sont allés diffuser de la publicité pour un magazine qui parlait de leurs actes. Le Brésil est un vrai nid à pirate avec pour le moment plus de 500 défaceurs actifs.

Cible : robots.mit.edu
Auteur : Silver lord
Commentaire : Retour de ce groupe brésilien qui, sur le site robotique du Massachusetts Institut of Technologies, signe son retour. Côté message, toujours le vide total, mais le but ne semble pas être de causer.

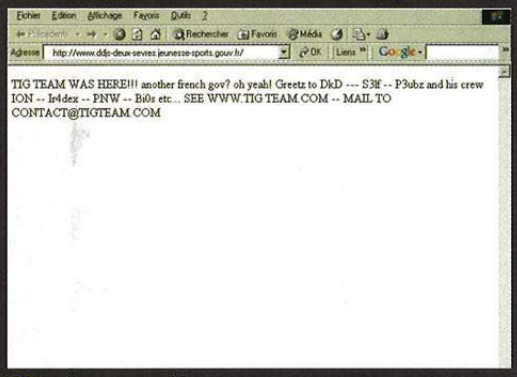


Cible : Bouygues Telecom
Auteur : DKD
Commentaire : Bouygues Telecom n'a pas dû apprécier l'humour. L'ensemble de ses serveurs web ont été piratés, et plusieurs fois de suite. D'abord par DKD, qui est allé passer son message anti-guerre. Dans la foulée, un autre pirate, d'origine marocaine, a "redefacé" le serveur expliquant qu'il trouvait lamentable de tels actes.



Cible : Americanintelligence.us
Auteur : HAW
Commentaire : Le site American intelligence est dédié au fan de renseignement militaire. Le groupe H.A.W., alias Hackers Against War, a souhaité mettre un peu de sel dans les pages de ces va-t-en-guerre. Un message contre la guerre et la politique de George W. Bush.

Cible : Iga
Auteur : Shadow Boys
Commentaire : Ce site appartenant à la marque IGA, des épiceries, a souhaité faire son malin entre les tomates et petits pois. L'histoire ne dit pas si le pirate a eu accès à la boutique Online. Espérons que non.



Cible : Gouvernement fr
Auteur : Shadow Boys
Commentaire : Voilà qui va remplir le dossier du juge. Le groupe TIG, comprenez Terminale Informatique et Gestion, a frappé sur plusieurs sites du gouvernement français : concours-civils.defense.gouv.fr - ddjs-deux-sevres.jeunesse-sports.gouv.fr - cote-dor.pref.gouv.fr.

DO YOU NEED DOMAIN NAME REGISTRATION AND DNS MANAGEMENT

WITHOUT UNEXPECTED RESULTS ? »

» eurodns

Noms de domaine européens
DNS-hosting gratuit

www.eurodns.com

Iliad et l'odyssée du web

Ce n'est absolument pas une blague : la société ILIAD souhaite faire disparaître de la circulation tous les sites dont le nom de domaine contient le terme « annu ». Nous sommes tous des particuliers, gérant des sites gratuits et n'ayant absolument pas les moyens financiers de nous défendre juridiquement face au mastodonte qu'est ILIAD, c'est pourquoi nous avons besoin de votre soutien !

Réponse : Que le web prend une étrange tournure ! La société Iliad, qui n'a pas souhaité répondre à nos questions, est propriétaire, entre autre, du 3617 annu, un service Minitel d'annuaire inversé, service décliné sur le web avec annu.com. Ils vont se marrer quand des centaines de sites vont afficher le mot annu sur leurs sites ou dans les méta-tags. Scandaleux ! Ne vous inquietez pas, il s'agit surtout d'une tentative d'intimidation, non fondée juridiquement parlant !
Pour en savoir plus : annu-secours.org/danger.html

Favoritisme !

Alors je ne comprends pas, dans votre magazine papier vous mettez Amen.fr dans la page des sites hackés en oubliant leur principal concurrent à savoir Ovh ? Vous avez bien en quelque sorte écrasé Amen.fr. Est-ce parce que vous êtes client Ovh ? Avez vous peur de les discréditer ou alors faites-vous de la rétention d'information (bizarre pour un journal de hacking) dans le but d'écraser Amen ?

Anthras 429 par Internet

Réponse : Nous n'avons pas souhaité écraser Amen, nous avons juste constaté le piratage. Pour OVH, pas de favoritisme, ils vivent, eux aussi depuis quelques temps une série de piratages allant de la modification de page en passant par le DoS. Pour ce qui est de clientélisme, pas de ça chez nous, en plus je suis moi-même client chez Amen et Ovh. Pour finir, ZATAZ Magazine n'est pas un journal de hacking, mais un magazine traitant, entre autre, de ce sujet.

Base de données, donnée

J'ai effectué sur le moteur de recherche Alexa (www.alexa.com) une recherche (backoffice superbonplan). En regardant les résultats obtenus, je me suis rendu compte que le site SUPERBONPLAN.COM a laissé en accès libre une partie de leur site qui contient un listing d'adresses e-mails : plus de 100.000 adresses ! Il n'y avait pas de mot de passe et ce listing aurait pu entraîner l'émission de mels non sollicités.

Ludovic - Paris

Réponse : Le problème est que de plus en plus de base de données sont ainsi accessibles d'un clique de souris. Heureusement, ici, cette société a corrigé rapidement son erreur. Il faut savoir que la loi française protège les internautes qui fournissent des informations comme leur mel. La CNIL et la loi informatique et liberté punissent ce genre d'erreur. A noter aussi que le spam, la publicité non sollicitée, est passible des peines prévues aux articles 226-18 (jusqu'à 300 000 euros d'amende et 5 années d'emprisonnement) et 226-24 (peine d'amende multipliée par 5 pour les personnes morales) du Code Pénal.

Démo'niak

Ca concerne le Hors série de Zataz "spécial copie". Juste pour vous remercier d'avoir fourni pleins de super productions provenant de la démo scène sur le CD. Il ne faut pas que ce mouvement disparaisse et je pense que grâce à vous des gens vont découvrir ce qu'est cette scène. Merci encore. (Greetz to 3state, acme, cocoon, delirium, eclipse, farb-rausch, future crew et les autres).

@vLaD13# de la planète Mars..eille

Réponse : Merci du compliment ! Votre humble serviteur a fait parti d'un des groupes cités :) Il est normal que nous soyons aussi passionnés par la scène démomakers. On compte bien continuer. Pour mon cas cela fait bientôt 15 ans que je baigne dans la démo. Autant dire que j'ai l'intention de finir dans la tombe avec 10 Tétras de démos !

Publicité par MSN

Salut ! C'est nouveau ce genre de bêtise ? C'est la première fois que je reçois un spam par MSN !

Doxical - paris

Réponse : Malheureusement oui ! Une nouveauté qui n'a pas fini d'énerver la planète si on n'y prend pas garde et surtout si Microsoft tarde à sortir un patch. Cette forme de publicité est apparue fin mars. Elle a été utilisée par des pirates souhaitant donner leurs avis sur la guerre en irak aux "méchants frenchies"...

Prudence !

Voila nous ne sommes pas encore le 30 avril et j'ai déjà un avertissement pour ma page perso qui se trouve chez AOL. Mon site a à peine 3 semaines. J'ai téléphoné et on m'a expliqué que mon contenu ne convenait pas et que je n'avais pas le droit de faire de la publicité pour d'autres sites.

Freddy - Lyon

Réponse : Nous avons contacté AOL qui nous a précisé que le contenu d'une page perso ne peut pas contenir d'informations illégales, à caractère pornographique ou diffamatoire par exemple. Notre lecteur ne semblait pourtant pas faire parti de ce genre de catégorie sauf que dans ses liens, deux sites proposaient des logiciels pirates. Donc méfiez-vous des liens que vous fournissez, même si ces derniers n'ont rien à voir avec votre site.

Beau comme un camion

Bonjour,
Je me demandais si vous n'aviez pas l'intention de vendre des tee-shirts, des casquettes aux couleurs de ZATAZ Magazine. Famille Betrand - Marseille.

Réponse : Nous n'avons pas l'intention de nous lancer dans du prêt à porter :) mais nous proposons depuis 1 an, avec la boutique 00Z00, une vingtaine de tee-shirts différents pour pouvoir frimer sur les plages cet été ! Voyez dans les liens sur zataz.com

Abonnez-vous à Zataz Magazine

et recevez un le CD Zataz Tools en cadeau !

6 n°s > France : 10 Euros - Belgique : 12 Euros - Suisse : 20 CHF - Dom - TOM: 20 Euros

OUI, Je m'abonne à **Zataz Magazine**

☐ **6 numéros**, je joins mon règlement de 10 Euros TTC.
Belgique : 12 Euros - Suisse : 20 CHF - DOM/TOM : 20 Euros

☐ **2 ans** (12 numéros), je joins mon règlement de 19 Euros TTC.
Belgique : 22 Euros - Suisse : 38 CHF - DOM/TOM : 38 Euros

Bulletin à renvoyer à :
Mediastone
61, rue Jouffroy d'Abbans
75 017 Paris

Je règle par :

> Chèque bancaire ou postal, à l'ordre de Mediastone.
> Carte bancaire Visa ou Eurocard n° ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐
Expire fin ☐☐ ☐☐

Nom _____ Prénom _____
Société _____
Adresse _____
Code Postal _____ Ville _____ Pays _____
Signature obligatoire :

En Cadeau

Le CD Outils Zataz (valeur : 15 Euros)

Un CD bourré à craquer d'utilitaires de sécurité !

(détails du contenu du CD ici : www.zataz.com/zataz/boutique.htm)

GLOSSAIRE

Appz :
Terme désignant des applications piratées, vient de l'association entre "apps" diminutif de "application" et de "warez", il existe aussi "gamez", "ftpz", etc...

Arpanet :
Ce réseau expérimental a été mis en place par l'armée américaine, sous l'égide du DARPA. Dès 1969, ce petit Internet avait pour but la transmission de données par paquet. L'idée était de palier les problèmes de communication en cas de conflit nucléaire. Les premiers protocoles de l'Internet y seront testés.

BSA :
Business Software Alliance. Association américaine de lutte contre les pirates de logiciels.

Board :
Autre terme désignant un BBS, ou alors un forum des news sur internet.

CERT (Computer Emergency Response Team) :
Centre d'étude et de recherche lié aux problèmes de sécurité informatique. Créé en décembre 1988 par la DARPA suite à la diffusion d'un virus qui bloquera, en novembre de la même année, 10 % des ordinateurs connectés au réseau.

CNIL :
Commission Nationale de l'Informatique et des Libertés. Veille au respect des lois françaises concernant l'informatique, ainsi qu'à la légalité des fichiers nominatifs et de leur utilisation - application de la loi 78-19 de janvier 1978 relative à l'informatique, aux fichiers
et aux libertés.

CSS :
Le CSS signifie Cross Site Scripting, à ne pas confondre avec le langage Cascade Style-Sheet. La vulnérabilité Cross Site Scripting affecte les sites web où il est possible d'entrer du texte dans des cases : Moteur de recherche, formulaires, forums, url, ... la faille fonctionne en insérant une ligne de code en langage JavaScript, VBScript à la suite d'un url par exemple. Les serveurs non protégés interprètent le code et l'exécutent. Les résultats sont nombreux, affichage d'un texte, vol de cookies, ...

DARPA :
Defense Advance Research Project Agency. Cette agence américaine dépend du secrétariat de la défense américaine.
Ils sont à l'origine, entre autre, de l'ARPANET.

Demomaker :
Il est passé du bon coté de l'underground informatique. Il réalise des démos, intros (de crack...). Chez les demomakers on y trouve graphistes, musiciens, codeurs, etc... Une démo est une expression artistique informatique. Ils se réunissent dans des démos party (The Party, Volcanic party, etc...) où en un temps fixé doivent produire une démo.

Flatrate :
Fournisseur d'accès à l'internet proposant la connexion au web et les communications illimitées dans un même pack.

La FTC :
Federal Trade Commission.

FAI :
Fournisseur d'Accès à Internet.

Firewalls :
Filtre entre plusieurs machines. Sert à protéger un réseau d'éventuelle attaque extérieure. Filtre et contrôle les accès.

Godfrain :
La Loi Godfrain, votée le 5 janvier 1988. Cette Loi relative à la fraude informatique a créé des infractions spécifiques en la matière, reprises par les articles 323-1 à 323-7 du nouveau Code Pénal institué par la Loi du 22 juillet 1992 entrée en vigueur le 1er mars 1994.

IP :
Internet Protocol. Standard utilisé pour l'adressage de données sur internet. Chaque ordinateur est connecté à une adresse IP qui lui est propre.

In the wild :
Un virus "In the wild" signifie que le virus s'est répandu.

PGP (Pretty Good Privacy) :
Programme de cryptage. Son auteur se nomme Philip Zimmermann. Il utilise une clé publique et une clé privée pour sécuriser vos messages. PGP est l'un des programmes les plus utilisés sur le web.

Taz :
Tempory Autonomous Zone. Tiré d'un concept du journaliste américain Hakim Bey. Le web et son contenu sont autonomes à un moment donné pour disparaître ensuite. Nous avons transformé l'Autonomous par Anonymous et fabriqué un Palindrome qui a donné le nom de notre magazine : ZATAZ.

Virus :
Programme informatique utilisant la plupart du temps un bug dans une machine afin de se reproduire, bloquer, détruire ou détourner des informations de l'ordinateur infecté par ce virus.

Virii :
Pluriel de virus. Un virus, des virii.

Vulnérabilité :
On appelle aussi trou de sécurité. Synonyme de faille ou encore brèche.

Ver :
A la différence des virii, le ver n'a pas pour but de se multiplier sur un même ordinateur. Son but est d'infecter le plus grand nombre de machines et donc de se propager. Il existe plusieurs catégories de ver. La plus connue, car nocive, se nomme mass-mailers, qui a pour but de s'auto-envoyer à un maximum de personnes. Pour cela le ver va utiliser le carnet d'adresse de la victime.

Warez :
Logiciels piratés.

Zombie :
Un ordinateur "Zombie" est en fait un ordinateur piraté qui va servir, à l'insu de son propriétaire à des actes de piratages. Les "zombies" sont utilisés par exemple dans une attaque de type DoS. Les machines "Zombies" vont officier à l'insu de leurs propriétaires respectifs afin que ces machines envoient des millions de messages en direction des serveurs-cibles ou des routeurs qui aiguillent le trafic. Une machine Zombie permet de créer plusieurs attaques, rendant la traque du pirate difficile.

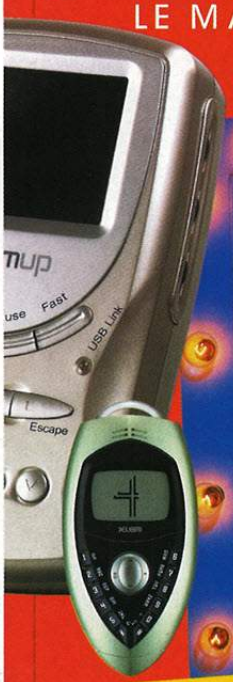
Le N°1 de la presse Internet !

Nice People : déja du contenu torride diffusé sur internet !

3.90€ N° 58 / Mai-Juin 2003

Net@scope

LE MAGAZINE DE TOUS LES INTERNAUTES



ACCÈS ADSL

Les meilleurs et les pires fournisseurs

EXCLUSIF !

Télévision par ADSL

On a essayé !

Protégez votre site des pillards

Webguide

Plus de 100 bonnes adresses

HIGHTECH

SPECIAL GADGETS

10 astuces pour être au top dans Google, Interview de Kevin Warwick, l'homme-Cyborg, toute l'actu du Web...

Le N°1 de la presse Internet !

OMINFO.COM

http://www.ominfo.com

Action Replay 2 V2

13.90 €

VGA Box Universelle

89 €

Carte Mémoire Game Cube 4 MB

29.65 €

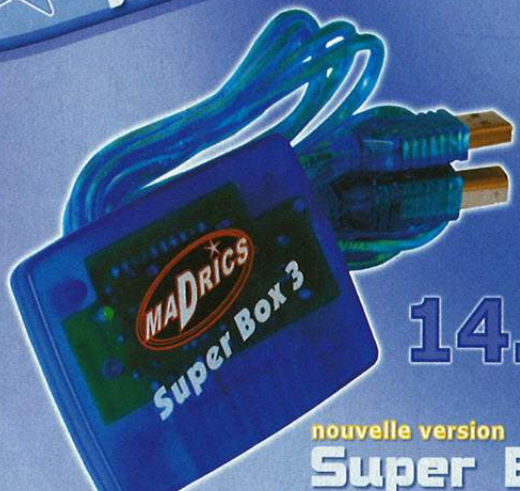
Tout l'univers des jeux vidéo !

5% de remise pour les lecteurs de ZATAZ avec le code ZATX429

offre valable jusqu'à parution du prochain numéro de ZATAZ

Pistolet PS2 Headhunter

31.90 €



14.90 €

nouvelle version

Super Box 3

Jouez sur PC avec vos manettes Playstation !

Une console à gagner par mois !

ALLO COMMANDE

03 25 32 24 37

CARTE BLEUE VISA EUROCARD MasterCard Diners Club International AMERICAN EXPRESS

Paiement en ligne sécurisé

FIA-NET.com ACHATS 100% GARANTIS

OMINFO.COM · BP 207 · 52006 CHAUMONT CEDEX · 03 25 31 47 28 · Fax 03 25 31 69 79

Réalisation AXESS MEDIA - http://www.axess-media.com