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

ZATAZ MAGAZINE

Bimestriel - Belgique : 2,3 Euros - Suisse : 4 CHF
n°3 Juillet - Août 2002

XBOX

Tous les jeux piratés

2€

Rendez vos CD incopiables

VAREZ

CE QU'ON NE VOUS DIT PAS
Special Copie de logiciels

Tout télécharger : jeux, logiciels...

Piratage de F1

Les pilotes conduisent-ils vraiment leurs voitures ?

M 05129 - 3 - F: 2,00 € - RD

Le magazine **Net@scope** passe en grand format

Découvrez le plus populaire des magazines Internet

n°3 Sommaire

EDITO

EDITO

Amis lecteurs, Bonjour ! Vous avez déjà dans les mains la troisième édition de Zataz Magazine. Vous avez pu le remarquer, nous venons de passer bimestriel et cela grâce à votre accueil plus que chaleureux. Dans ce nouveau numéro, du 100% exclu, comme toujours ! Avec toute l'actualité, un reportage inédit et exclusif sur les vrais réseaux de la contrefaçon de logiciels (vous y découvrirez que ce que l'on nous raconte est loin de la réalité), un spécial Xbox et les pirates, totalement inédit avec l'interview exclusive d'un des fondateurs du groupe Messiah, les auteurs de la première puce Xbox underground. Côté technique on vous a dégoté de quoi être fier devant votre machine. D'abord des trucs et astuces totalement inédits pour Windows ou encore comment protéger vos CD-Roms et CD Audio face aux pirates. Deux Interviews exclusives pour finir, dont celle du groupe de Hackers Deceptive Duo, qui a mis en boule les services secrets américains. On vous laisse découvrir les autres articles et rubriques. Bonne lecture.
On se retrouve début septembre !
Damien Bancal

PS : odqqnm wjmbjo onmdtq

une publication
MEDIA Stone
http://mag.zataz.com

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

Chef de la rédaction : Damien Bancal
Ont collaboré à ce n° : Benoit Guignard, Eric Romang, Antoine Santo, LaurentZ, Geek Girl, Jasper, Webmaster guerreco.com
Merci à ARTCH et Christophe GAUTHIER pour leurs créations graphiques.

Impression Leonce Deprez, Béthune
Distribution : NMPP **N° de Commission paritaire :** En Cours. Dépot légal à parution.

Magazine édité par : Mediastone
Directeur de la Publication : Charles Daleau
Siret : 42990015200019 -
Code APE : 221 E

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

actu!

Toute l'actualité du hacking et du piratage !

Planète Underground

ROGUE WARRIORZ

Un nouveau réseau de pirates de logiciels a été stoppé mi-juin par le FBI. 21 personnes ont été arrêtées dans 14 états, ainsi qu'au Canada. Ils n'ont pas été mis en prison mais ils vont devoir comparaître devant le tribunal de Las Vegas. Lieu symbolique pour un grand nombre de pirates, c'est dans cette ville, début août, que se déroule le Defcon, meeting annuel à la sauce yankee. 21 personnes soupçonnées, plus de 8 000 logiciels saisis et quelques 350 films, bref une broutille chiffrée à sept millions de dollars. Les pirates risquent cinq ans de prison et 250 000 dollars d'amendes.

JPEG VIRAL

Plusieurs sociétés d'antivirus ont découvert un nouveau virus qui se communique par le biais d'images digitales. Ils ont nommé cette bestiole JPEG infector - W32/Perrun. Le virus fonctionne en deux étapes : Le fichier jpeg devient infecté puis un autre virus se charge d'extraire la partie virale de l'image. Bref, beaucoup d'infections et de bruit. Ce virus est plus une curiosité numérique qu'une véritable menace !

MORT D'UN HACKTIVISTE

Le 2600 est en deuil. Jack Biello est décédé début juin d'un cancer. Il a été l'un des plus actifs défenseurs de Kevin Mitnick, le premier pirate informatique médiatisé. Il avait créé, à l'époque, le site freekevin.com et kevinmitnick.com. Il s'était donné comme but d'aider Mitnick en prison, ainsi que lors de sa remise en liberté. Nous l'avions rencontré l'année dernière à New York.

DECSS ILLÉGAL

Le magazine américain 2600 a perdu son appel au sujet de la décision de rendre illégalles toutes informations dédiées au système de déchiffrement des DVD, le fameux code DeCSS. La deuxième Cour d'appel régional de New York maintient que DeCSS viole directement la loi sur le Digital Millenium Copyright Act.

Le film Matrix sur GBA

Nous vous expliquions dans ZATAZ Magazine papier numéro 2 comment fonctionnent et où se trouvent les nouveautés Divx sur Internet. Nous racontions aussi comment certains pirates chinois s'amusent à mettre des films sur la petite de Nintendo, la Game Boy Advance. On vous propose maintenant de regarder la bande annonce du film Matrix. Pour cela téléchargez un émulateur GBA et il ne vous restera plus qu'à halluciner !
ftp://ftp2.zataz.com/zataz/Demomakers/Demos_GameBoy/matrixgba.zip

Sony n'est pas chien

En Octobre 2001 Sony avait demandé au webmaster du site Aibohack de stopper la diffusion d'informations permettant de modifier son chien-robot Aibo. Sony avait déclaré que le programme de son robot en plastique était sous copyright. Aujourd'hui Sony change sa laisse d'épaule et autorise la modification de son chien pour que les utilisateurs puissent le rendre encore plus vivant. Sony va même proposer un kit gratuit de sorte que les propriétaires d'Aibo puissent lui enseigner de nouveaux tours. Un site web va être lancé pour y placer les contributions des codeurs poilus ! On attend avec impatience l'option qui fera hurler Aibo comme Scoubidoo !

XBOX underground

Il est possible de jouer aux jeux XBOX via le web ! De nombreux joueurs en ont eu marre d'attendre la mise en place du futur réseau Xbox Live et se sont lancés dans le pari, réussi, de jouer on-line sans l'avis de Microsoft. La société GameSpy vient d'ailleurs de mettre en ligne un logiciel permettant de jouer à Halo en réseau, via votre PC.
http://www.gamespyarcade.com/download/

Warez sur Game Cube

Plusieurs magazines dans le monde ont annoncé que la console de Nintendo, la GameCube version Q vient de voir ses premiers jeux piratés. Il parait, cependant que les marchés européens et américains ne seront pas touchés par cette fraude, vu que le produit n'est pas disponible sur ces deux continents. Il semble donc qu'avec des Q modifiés, il est possible de lire des jeux copiés sur DVD-R. Ces DVD ne coûteraient que 15 euros. Certains magazines vont même jusqu'à citer les jeux piratés : Super Monkey Ball, Star Wars, Extreme GIII Racing et Hyper Sports 2002 Winter.

Protection à la con ?

Imaginez. Vous êtes une énorme major. Vous venez de claquer plusieurs millions de dollars pour protéger vos albums musicaux des pirates. Vous annoncez cette découverte à toute la presse. Vous êtes content, la protection marche pas trop mal, les investisseurs et actionnaires sont heureux. Vous allez pouvoir vous goinfrer de dollars encore plus qu'avant. Seulement voilà. Vous pensez que les hackers sont aussi méchants que les pirates et vous n'avez pas voulu leur faire confiance. Il vous avaient pourtant dit que la protection magique avait quelques failles. Vous n'avez pas écouté et aujourd'hui vous voilà avec une protection qui ne tient pas la route. Il suffit en effet d'un petit bout de Post-it pour contrer le système anti-piratage utilisé par Sony pour protéger ses albums. Un simple coup de marqueur pour CD sur la clef anti-copie, la partie la plus claire à la base du disque, suffit aussi pour contrer cette protection. Voilà qui est fâcheux. Les pirates vont pouvoir aussi raturer le texte sur le CD qui indique : "Ne fonctionnera pas avec un PC ou un Mac". On rappelle que de ne pas respecter les droits d'auteurs peut entraîner la disparition de la créativité et l'augmentation du prix des albums.

Oeil pour œil

Voilà le nouveau jeu lancé par le site web cryptome : référencer en photos les agences et structures secrètes appartenant à la CIA, FBI et la NSA. Pour y "jouer", les internautes utilisent l'outil GlobeXplorer qui permet, avec un simple adresse postale de zoomer sur des lieux et bâtiments. On doute que l'Oncle Sam n'est pas eu la maîtrise des images diffusées sur le web via Globexplorer. Un exemple d'image, le CIA Office of Special Technology, base dite secrète de la C.I.A. chargée de la fabrication d'outils d'écoutes, d'espionnage, et de destruction.

LOGICIEL

KryptoCom propose des fonctionnalités complètes de cryptographie (chiffrement AES, RSA, compression, Hash...) (exemples avec code source et documentation en français). Ce composant est compatible avec de nombreux langages tels que C/C++, VBscript, Visual Basic, Delphi, JavaScript, Java etc... il est disponible sur le site de Protek-lab en version démo sans limitation de durée. Nous faisons le lien sur zataz.com

SO BRITISH

Le Ministère des Affaires Etrangères britannique a admis qu'un courrier électronique donnant les détails secrets d'une visite du Prince Charles en Pologne a été... mal adressé. L'e-mail contenait les détails de son déplacement ainsi que les véhicules qu'il allait utiliser dans ses déplacements. Du pain béni pour les terroristes.

MILLE ET UNE NUIT AU POSTE

Il ne faut pas être très malin pour vendre des contrefaçons que l'on trouve gratuitement sur le web. D'autant plus que les copies de films sur CD ROMS que les gendarmes ont saisi étaient vendues sur les marchés aux puces. Les gendarmes de Bully-les-Mines, dans la région de Lens ont arrêté jeudi un homme, qui avec 1 000 copies illicites, sur DVD ou copiées sur des cassettes VHS, se faisait de l'argent de poche sur les marchés aux puces de la région. D'après une source proche de l'enquête, l'individu arrêté serait l'une, voir la tête pensante du trafic.

BENJAMIN, LE VIRUS KAZAA

L'outil d'échange on-line Kazaa a eu de la visite ce week-end. Un virus, nommé Benjamin, a tenté d'infecter les membres de ce réseau de peer-to-peer. Ce virus agit de manière assez efficace. Il va créer une liste d'adresses accessibles par d'autres membres du réseau Kazaa. Il ouvre ensuite une page web bourrée de publicités. Bref son auteur ne va pas être difficile à trouver, il faut juste demander à la régie pub qui doit être payé !

actu!

Toute l'actualité du hacking et du piratage !

Planète Underground

POLICIER BELGE PIRATE

Voilà une histoire belge comme on en n'a jamais entendue encore. Un policier belge, de la ville de Mons, a été arrêté pour avoir piraté une société informatique basée à Bruxelles. Le policier a simplement piraté l'entreprise concurrente de sa femme pour y voler des documents. "Il voulait se prouver qu'il était capable de le faire et souhaitait montrer à un client que l'entreprise adverse n'était pas sécurisée" dixit une source proche du juge d'instruction, Me Claise, qui a en charge cette affaire. Le policier risque 3 ans de prison.

ACTION INNONCENTE

L'association "Action Innoncente" est un regroupement de personnes qui se sont donnés pour but la lutte contre la pédophilie et la pornographie impliquant des enfants sur Internet. Le travail de cette association consiste principalement à faire de la prévention auprès des adultes et des enfants grâce à un site Internet, une BD, un conte et prochainement un jeu sur le réseau... Basée à Genève en Suisse les lecteurs helvètes peuvent contacter cette association via notre lien sur Zataz.com. Pour la France, nous ne pouvons que vous conseiller de joindre le Bouclier.org

EMPÊCHER AIM+ DE VOUS ESPIONNER

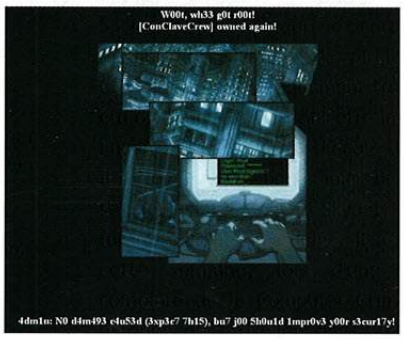
Voici une petite méthode pour calmer les ardeurs de curiosité du Messager d'AOL. Cette information a été diffusée par Pedram Amini de Tulane.edu. AIM+ est un Add-On non officiel pour Aol Instant Messager. Il envoie régulièrement des informations à propos de votre ordinateur à son site web. Pour empêcher cela, procurez-vous un éditeur hexadécimal et ouvrez AIM+.dll dans votre dossier d'installation d'AIM+, il vous est fortement conseillé d'en faire une copie. Recherchez la chaîne de caractère "tracking" ; une URL doit la suivre ; remplacez cette URL par des caractères nuls. En cas de problème, utilisez votre copie de remplacement. Il est possible que l'éditeur, dans une prochaine version, cache un peu mieux son espion.

Il y a comme une fuite...

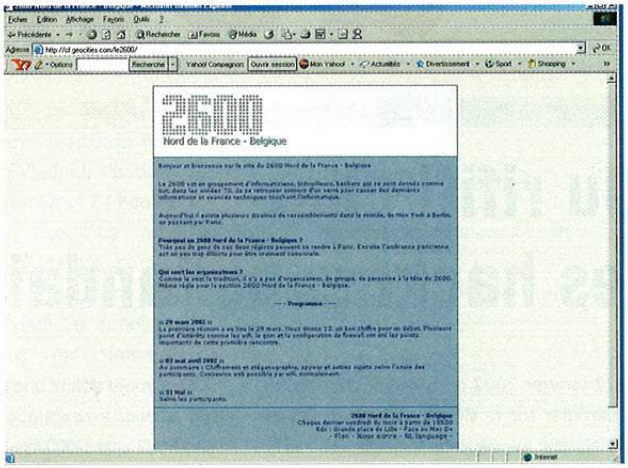
Il y a comme qui dirait une fuite chez Infogrames. La version démo jouable de Unreal Tournement 2003 est déjà diffusée sur Internet. Seul hic, ce n'est pas le service presse d'Infogrames qui la diffuse, celle-ci n'étant attendue que dans quelques semaines, mais un groupe de pirate nommé RDMiSO. Fake marketing ou véritable fuite ? On peut se poser la question. Lorsque l'on lance cette démonstration, un texte en haut de l'écran, notifie ceci : " UT2 release - Private and Confidential / (c) 2001 Digital Extremes". A suivre...

L'orage tombe sur Skynet

Sacré diable rouge que ce Scorpio. Il était membre d'un groupe de pirates nommé ConClavCrew. Techniquement très fort, il a cru du haut de ses 18 ans être intouchable. Encore au lycée, vivant du côté de Louvain, il a décidé un beau jour de mars de s'attaquer au réseau de Skynet, le premier fournisseur Internet Belge. Il a été arrêté cette semaine, lors d'une opération conjointe de la Computer Crime Unit du parquet de Bruxelles, la CCU et de la Computer Crime Unit fédérale. Le pirate voulait entrer dans le réseau. Pour réussir il s'est attaqué au portail Internet de Skynet, le talon d'Achille de cette société. Il a réussi à voler pas moins de 18 000 comptes clients mais sans provoquer de gros dégats aux dires de Skynet qui conseille tout de même à ses membres de changer leurs mots de passe. Il risque de 6 mois à trois ans d'emprisonnement. La police belge aura mis



15 jours pour attraper le jeune pirate. Un nouveau nom sur un tableau de chasse bien garni après le démantèlement, il y a quelque mois, du groupe BHZ. Pour Skynet, après l'effacement "par erreur" de sites web de ses abonnés, la diffusion d'un virus dans un cadeau envoyés à ses membres et finalement ce dernier coup montrent que ce genre de géant n'est jamais à l'abri de rien.



Meeting 2600

Le 2600 est un groupement d'informaticiens, bidouilleurs, hackers qui se sont donnés comme but, dans les années 70, de se retrouver autours d'un verre pour causer des dernières informations et avancés techniques touchant l'informatique.

La région du Nord de la France, ainsi que la Belgique n'avaient pas leur regroupement. Voilà qui est fait. Le 2600 Nord de la France est organisé par des étudiants de plusieurs écoles informatique de la région.
http://cf.geocities.com/le2600/

Chaud devant !

La société coréenne Woksdome a offert 100 000 dollars aux "hackers" qui pouvaient laisser leur pseudo sur la page de garde ce cette entreprise spécialisée en sécurité informatique. Le concours aura duré 15 heures. Des messages de hackers se sont ainsi retrouvés un peu partout sur le site... Exemple de phrases laissées dans la page index : "Xpl017Elz was here. P.S: I was owner for a long time. :-)" ou encore dans la page Registration : "Hey guy" content="You are not so secure... hacked by... WHO KNOW??? Italian do it better! uaz uaz uaz, playhouse rules". Bref cette société va réfléchir à deux fois maintenant avant de lancer un concours.

MAIL BOMBING QUI MAL Y PENSE

La 12ème chambre du TGI de Paris a condamné un informaticien de 29 ans pour avoir envoyé 300.000 e-mails afin de bloquer le fournisseur Internet Noos. qui a vu sa messagerie bloquée pendant 10 heures. L'auteur de l'attaque est tombé sous le coup de la loi Godfrain qui indique qu'il y a eu "entrave au fonctionnement d'un système de traitement automatisé de données." Le jeune homme a été condamné à 4 mois de prison avec sursit et à 20 000 euros d'amendes.

OUTLOOK INTERDIT

Le collège britannique de Newnham va faire interdire l'usage d'Outlook car l'administrateur en à plein le dos de se coltiner les centaines de milliers d'e-mails infectés que peut recevoir son école. Juste un détail, l'école va continuer à les recevoir mais n'infectera plus les machines de l'écoles, "God save the net".

SOURIEZ, VOUS ÊTES LOGGUÉS

Deux tiers des parlementaires européens ont adopté le principe de "la rétention des données" privées. En gros comprenez qu'il va bientôt être possible, comme le KGB ou la Stasi en leurs temps, de surveiller et exploiter les communications électroniques. Attention, ici on ne parle pas que d'Internet, mais aussi du téléphone, ...

UNE VENTE QUI FAIT BOOM

Un tribunal californien a condamné à 10 mois de prison, 2000 dollars d'amende un homme de 22 ans qui vendait aux enchères sur Ebay des explosifs alors qu'il n'avait pas l'autorisation requise pour le faire. Le gars envoyait ses créations par la poste. (Source : Me Cahen)

TENNIS

Stefi Graf a gagné un procès contre Microsoft Allemagne. De fausses photos de nus la représentant étaient visibles sur un site contrôlé par Microsoft. Le tribunal a jugé que Microsoft Allemagne était responsable du contenu de son site et devait s'assurer de l'absence sur son site de ce type de photos.

actu!

Toute l'actualité du hacking et du piratage !

Planète Underground

VIRUS SQL

Un nouveau virus cible le logiciel de gestion de données SQL de Microsoft. Le ver attaque via le port 1433 et d'après SANS, institut dédié à la sécurité informatique, ce code malicieux a déjà touché plusieurs dizaines de milliers de serveurs. Nous vous parlions voilà quelques semaines d'étranges attaques vers le port 1433. Nous avons donc aujourd'hui la réponse à nos interrogations.

SACRÉ KIM

Fin du feuilleton d'un mythomane. Kim Schmitz, alias Kimble, vient d'être condamné par le tribunal de grande instance de Munich à 20 mois de prison avec sursis et 100.000 euros d'amende. Nous relations la vraie vie de ce pirate pas comme les autres dans ZATAZ Magazine papier n°2.

VOLEUR NUMÉRIQUE

Il commence à être connu le Zilterio, nous avons déjà parlé sept fois de ce personnage qui n'a rien de virtuel. Ce pirate a une spécialité : vol et chantage à la base de données bancaires. La société Thenerds.com est la nouvelle victime de ce voleur qui n'hésite pas à réclamer de l'argent pour éviter de voir la base de données, qu'il a pu dérober, se retrouver dans la nature. Sa dernière trouvaille comporte tout de même pas moins de 150 000 clients. Il a déjà fait le coup à plusieurs grosses sociétés comme un provider californien ou encore à l'encontre de la société Web Certificates chez qui il avait demandé 50.000 dollars. Le pirate a été ciblé en Russie, en Malaisie ou encore au Yemen. Bref, nul part.

POUR UN DOLLAR T'AS PLUS RIEN

Après la fermeture du site Taiwanais Movie88.com, c'est au tour d'un site iranien film89.com de se voir couper par la Motion Pictures Association (MPA). Ce site web proposait à la location des films pour la somme de 1 seul petit dollar.

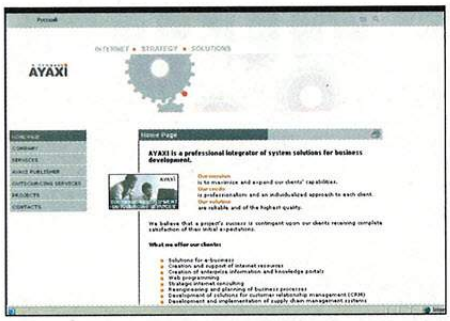
Du rififi chez les hackers hollandais

Le 22 janvier 2002 dernier, un chat devait se dérouler sur le site de la Maison Royale hollandaise (www.koninklijkhuis.nl) avec Maxima Zorreguieta, future Princesse des Pays Bas, qui épousera le 02 février de la même année le Prince Willem-Alexander. (NDR, voir ZATAZ Magazine 2) Le Chat devait porter sur le mariage et les intervenants du chat avaient été sélectionnés. Mais les vilains pirates s'en sont mêlés et ont bombardé le site, tenu par KPN (NDR : fournisseur équivalent France Télécom d'ici), d'attaques Denial of Services. Prêt de 3 milliards de demandes de connexion semble-t-il. Du coup, Le chat a duré quelques minutes. Un groupe, le "Down Under Crew " avait revendiqué l'attaque. Le "DUC" était composé de huit membres, âgés de 18 à 30 ans. Les gars expliquent qu'ils n'avaient rien contre le futur couple princier mais que KPN l'aurait trop "ramené" en affirmant que le soir du chat : "tout serait blindé (...) impossible à pirater". Du coup le "DUC" a voulu donn2 une petite leçon à KPN. L'un d'eux a expliqué au journal "de telegraaf" que 3000 machines avaient été utilisées après les avoir contaminées avec un cheval de Troie. Les pirates en ont profité pour passer par "Cavemen" (www.cavemen.nl) hébergeur hollandais. Seulement, les pirates discutaient aussi via des canaux IRC de Cavemen. La police enquête et six personnes sont interpellées, fortement soupçonnées d'avoir participé à l'attaque. Sur l'affaire les Hollandais ont travaillé avec la police allemande, qui enquêtait pour d'autres affaires sur ce groupe et un autre nommé les "Xtreme Power - XP ". Là dessus, coup de théâtre, dans une emission sur la chaîne télé RTL Boulevard, un "hacker anonyme" balance deux noms des responsables du hacking de Maxima. Le responsable de l'émission est menacé... Dépôt de plainte et Bingo, un des "DUC" faisait partie de la première fournée d'interpellés.

My name is Satos

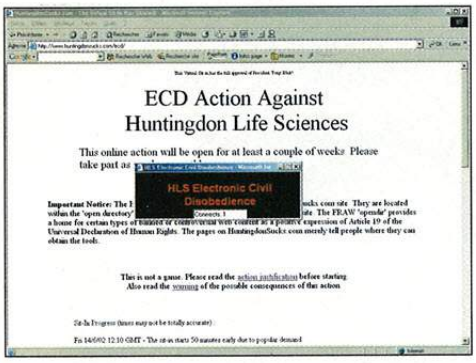
Duncan Campbell est l'homme par qui l'affaire Echelon a éclaté. Il traque le système d'espionnage des américains sur toute la planète. Il était, il y a quelques heures, en Suisse. Voici quelques photos que les amateurs de chocolats... et d'espionnage vont adorer ! Des antennes qui sont situées du côté de Loèche. La Suisse a lancé un projet nommé Statos qui doit permettre de prévenir toutes menaces liées à la technologie et au terrorisme. Duncan Campbell explique que Satos pourrait être un des maillons du système Echelon. Pour rappel, le 4 octobre 2000, Swisscom vendait à la société américaine Verestar ses antennes paraboliques de Loèche, Genève et Bâle.

Sacré Poutine



96 pirates informatiques ont essayé de pénétrer le nouveau site de Web du Président russe Vladimir Poutine, et cela dans les premières 24 heures de la vie du site. Le site president.kremlin.ru, serait, paraît-il, parfaitement protégé face aux pirates. En gros, voilà un appel du pied énorme pour voir comment agissent les pirates. Un Honey pot, un pot de miel, officiel, en quelque sorte. Environ 500.000 personnes ont visité le site depuis son ouverture. La société en charge de la sécurité du site se nomme AYAXI, elle est basée à Moscou. Ils auraient mis dix mois pour mettre en place le serveur de la présidence russe.www.ayaxi.com

Hacktivism



Imaginez. Vous êtes une énorme major musicale. Vous venez de claquer plusieurs millions de dollars pour protéger vos albums musicaux des pirates. Vous annoncez cette découverte à toute la presse. Vous êtes content, la protection marche pas mal, les investisseurs et actionnaires sont heureux. Vous allez pouvoir vous goinfrer de dollars encore plus qu'avant. Seulement voilà. Vous pensez que les hackers sont aussi méchants que les pirates et vous n'avez pas voulu faire confiance. Il vous avez dit pourtant que la protection magique avait quelques problème. Vous n'avez pas écouté et aujourd'hui vous voilà avec une protection qui tient pas la route. Il suffit donc d'un petit bout de Post-it pour contrer le système anti-piratage utilisé par Sony pour protéger ses albums. A noter qu'un simple coup de marqueur pour CD sur la clef anti-copie, la partie la plus claire à la base du disque pour contrer cette protection. Voilà qui est fâcheux. Les pirates vont pouvoir aussi raturer le texte sur le CD qui indique : "Ne fonctionnera pas avec un PC ou un Mac". On rappelle que de ne pas respecter les droits d'auteurs peut entraîner la disparition de la créativité et l'augmentation du prix des albums.

Sniffer dans une fac

L'université d'Etat d'Arizona a quelques soucis. La police du campus vient de découvrir que des logiciels espions, des sniffers, ont été placés dans les ordinateurs de la fac pour intercepter les frappes claviers. D'après les enquêteurs les logiciels étaient configurés pour intercepter les numéros de cartes de crédit des étudiants, des mots de passe ou encore les courriers électroniques. L'Arizona State University possède 20.000 ordinateurs et traite pas moins de 2 millions de courriers électroniques par jour. Plusieurs autres universités semblent avoir été touchées par le problème. Le programme espion a été retrouvé sur des ordinateurs d'accès destinés aux étudiants en Floride, en Arizona, au Texas ainsi qu'en Californie. La mafia russe est visée car les ordinateurs surveillés étaient liés à des IP basés en russie.

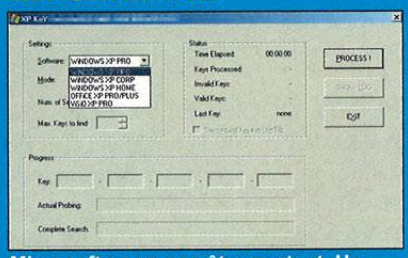
QUI VEUT LA PEAU DU 2600

Après avoir connu les juges, les tribunaux, voici que le chan IRC du 2600 est fermé par... des petits cons. Une attaque de Déni de Service, un DoS, a bloqué l'irc.2600.net, le chan du site officiel du 2600. "Notre hébergeur n'a pas cherché à comprendre et au lieu de tenter de se protéger a tout bêtement coupé la connexion". Triste de voir que l'un des plus vieux et plus respectés des groupes underground soit rendu muet par des gosses qui ne cessent de crier à la liberté d'expression. Quitte à prendre un pseudo, qu'ils prennent "pathétique" ça ira plus vite pour comprendre leurs motivations.

CARTES TV PIRATES

Quelques cartes pirates de télévision par satellite ont une étrange influence sur les ondes radios des services de secours canadiens. Il semblerait que ces cartes pirates créent des interférences sur les ondes hertziennes des radios employées par les services de police et de secours du canada. Un exemple a été donné, la Recherche Aérienne Civile et l'Association de Secours se sont retrouvées à rechercher non pas des personnes perdues, mais... des oies sauvages. "Certaines de ces cartes émettent sur les mêmes fréquences, ce qui peut occasionner de graves problèmes" dixit un policier du cru. A se demander si ce n'est pas la seule méthode qu'à pu trouver les fournisseurs de TV par satellite pour tenter d'inquiéter les consommateurs de ce genre de carte. (Source : Canada.com)

KEY GENERATOR



Microsoft ne va pas être content. Un outil est déjà en ligne pour créer des keys, comprenez des clés d'activations pour ses logiciels Office XP Pro ou pour Windows XP Pro. Cet outil permet d'installer XP Pro sur un nombre illimité de machine, ce qui est, normalement impossible.

Xbox, une cible

Depuis le début du mois de mai les pirates et autres bidouilleurs du fer à souder se sont lancés à l'assaut de la console de jeux de Microsoft. On avait jamais vu un tel engouement avec pas moins de 5 puces "pirates" dédiées à cette console. ZATAZ Magazine a été faire un petit tour du côté des hackers de Xbox.

Aujourd'hui les consoles de jeux ont envahies le marché et les pirates mettent les bouchées doubles pour proposer en premier des copies et le moyen d'en faire profiter les utilisateurs. Dernier cas en date, les contrefaçons pour la console de Microsoft, la Xbox. Le web regorge déjà d'émulateurs pour cette console. Mais, attention ils sont tous faux et contiennent à 99 % un virus voir pire, un cheval de troie, comme d'ailleurs les "boots CD", censés permettre de jouer avec une copie en insérant d'abord un CD faisant sauter la protection de la Xbox. Pour ce qui est de la copie des jeux pour cette console, la guerre entre pirates et créateurs de puces ne fait que commencer. Début Mai, deux groupes de pirates spécialisés dans les consoles de jeux annoncent avoir réussi à copier les premiers jeux Xbox. Les groupes se nomment Riot et ProjectX. Microsoft peut commencer à trembler.

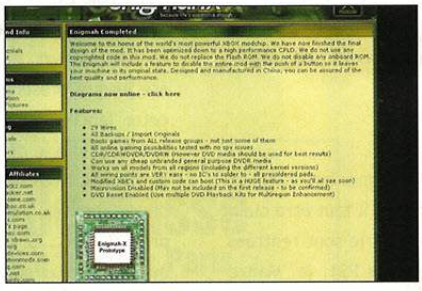
Puces, copies et vidéos

ProjectX est en fait un très grand groupe warez américain nommé Kalisto. Ils sont spécialisés dans les logiciels contrefaits pour la Playstation 2. Ils se sont associés avec une autre équipe appelée Echelon afin de mettre au point les copies pour Xbox. Dans tous ce bordel numérique les concepteurs de puces se battent dans l'ombre. Xtender et Neo technologie se disputent pour savoir qui sortira la première puce pour la XBox. Puce qui permettra bien sûr de jouer avec des copies. Cinq produits sont déjà sur le marché. La Xtender, la Neo X, l'Enigma X, la Pandora et la Messiah X. Bref, du jamais vu dans le petit monde des bidouilleurs de consoles. Les Xtenders ont d'ailleurs diffusé une vidéo début mai montrant la capacité de ce groupe à lire une copie de jeux Xbox. "Le grand public y croit mais sortiront-elles un jour ces puces et à quel prix ? On risque de voir des puces à plus de 100 euros avec plus de 30 fils à souder (...) Ebay va encore être rempli de Xbox "cramées" comme cela a été le cas avec les PS2. Les soudures sont très précises sinon c'est la fin de la console et direction poubelle" nous expliquera l'un de ces férus de bidouillage.

Bonjour les prix

Comptez 80 dollars pour une puce sur le marché des revendeurs alors qu'elle est vendue entre 35 et 45 dollars du producteur au revendeur. Belle marge ! Pour ce qui est des jeux, on les trouve à la pelle sur le réseau et quatre groupes s'arrachent les productions : Riot, Syndicate, Accession et ProjectX. Alors que Microsoft baisse le prix de son dernier jouet, il y a fort à parier que les juristes de Bill Gates ne vont pas laisser passer autant de moyens qui permettent de contrefaire et d'utiliser les jeux copiés XBox.
Comme l'écrivait Jean-Philippe Bay dans les colonnes de TF1.fr : "Dès le début, Microsoft avait annoncé que la vente de la console seule ne serait pas rentable, l'éditeur comptant sur la commercialisation des jeux pour dégager des bénéfices (...) Interrogé par nos soins à ce sujet, Microsoft France a indiqué avoir connaissance de l'existence de copies sur CD-Rom des jeux Xbox, mais selon la firme de Redmond, aucun ne peut fonctionner sur la console." Microsoft tente de minimiser le problème à défaut de le contrôler. Aux Etats-Unis les douanes tentent de faire ce qu'elles

de premier choix



peuvent et suivent au pied de la lettre le DMCA, comprenez le Digital Millenium Copyright Act. Les gabelous bloquent toutes les importations du site lik-sang.com, car ce dernier vend des puces pour toutes les consoles et est accusé par les ayant-droit d'être utilisé pour permettre aux possesseurs de consoles de jeux de jouer avec des copies pirates.

Opération à puces ouvertes

Il se nomme Bunnie, il est étudiant dans l'une des plus prestigieuses écoles scientifiques au monde, le MIT. Bunnie propose une page web nommée "bunnie's adventures hacking the Xbox" comprenez le décorticage de A à Z de la XBox : Electronique, code, bios, bref de quoi donner des sueurs froides à Bill Gates. ! web.mit.edu/bunnie/www/proj/anatak/xboxmod.html

Divx sur Xbox

Que de bonus pour la dernière console de Microsoft. Voici venir un programme qui va vous permettre de regarder vos films de vacances, codés au format Divx sur votre console Xbox. Le logiciel, nommé XboxDivx, pèse pas moins de 15 Mo. Certains amateurs de cette console, il y en a pas beaucoup, ont été jusqu'à remplacer le lecteur d'origine par un lecteur DVD Pionner, plus rapide et surtout moins capricieux à reconnaître les CDRW. Ce logiciel n'a rien d'illégal. Vous pouvez le télécharger sur mag.zataz.com.

Les puces attaquent !

Plusieurs groupes et sociétés viennent de sortir pas moins de cinq puces pour la console Xbox, grâce à Enigmah. Derrière ce nom se cache en réalité une alliance entres plusieurs sociétés, ayant des points de chute en France, Angleterre et Taiwan. Nous avons pu joindre Side, l'un des membres fondateurs du groupe.

Qu'est ce qu'Enigmah ?

Enigmah est le regroupement de plusieurs sociétés qui ont conclu un accord tacite après la période où certaines des sociétés aujourd'hui réunies sous la bannière Enigmah, se livraient une guerre sans merci concernant le marché des puces PS2 (NDR : des membres de Messiah avec d'autres codeurs de la team NEO ont sorti la puce NEO4). D'autres accords sont en cours, notamment une alliance et une association mondiale, dans le but de protéger, et d'aider lors de recours juridiques les membres de cette alliance et cette association. Enigmah est en fin de compte, le début de ce que l'on espère être, une reconnaissance de notre métier, notamment d'un point de vue juridique, il est inacceptable et complètement ridicule de voir de nos jours certains de nos contacts, membres, ou concurrents, sont traînés en justice, voir en prison. Enigmah s'ancre dans cette vision, celle d'une alliance permettant de fournir les meilleurs produits, en essayant de maintenir une grande confiance entre nos membres, ainsi qu'une rétribution des tâches de façon équitable, et bien entendu en garantissant du mieux que nous pouvons la sécurité de nos membres, notamment par rapport à la justice.

Pourquoi une puce Xbox ?

On ne va pas se voiler la face, c'est avant tout pour gagner notre vie, et aussi parce qu'on ne sait rien faire d'autre... La dessus il faut être clair, la plupart des personnes impliquées dans cette industrie sont rentrées dans ce milieu il y a 7-8 ans, au balbutiement de la PS1, le "Maître Spirituel" du mod chip, Scott Rider (NDR : pseudo Old Crow) fut le premier a fournir publiquement le code de la première puce PS1, tout est parti de là. Par la suite le non moins célèbre britannique Steve Hoyle, apporta des changements à ce même code, notamment les modes PHANTOM. D'autres ont suivi, et bien entendu se sont adaptés au marché. Apres la PS1 et la Saturn, ce fut le tour de la DreamCast, puis des lecteurs DVD, les graveurs de CD audio de salon, même des voitures et leurs boîtiers à injection. Dans ce domaine, d'autres sociétés sont déjà bien implantées et ne souffrent pas des mêmes problèmes que nous pouvons avoir par rapport à la justice. Aujourd'hui le marché de la PS2, du Nintendo GameCube et de la XBOX a ouvert de nouveaux horizons. C'est donc tout naturellement qu'après avoir participé au développement des puces PS2, nous nous sommes tournés vers la Xbox.

Difficile à créer ?

Non pas vraiment, tout dans la Xbox, est géré par le Bios. Les premiers kits de développement intégraient une copie du Bios d'origine, et ont très vite circulés sur le net. Nous avons très facilement pu isoler l'algorithme de cryptage, apporter les changements et les tester très facilement. Une simple XBOX avec un socket adéquat permet de tester les codes en quelques secondes. Une fois le BIOS qui répondait a nos demandes en main, il a fallu développer sur un composant tiers, un code qui allait patcher nos changements dans le bios d'origine. Chose réalisée en 3 semaines. En tout et pour tout, il nous a fallu 2 mois de développement. Ce qui reste un délai tout a fait convenable quand on sait qu'il a fallu prêt de deux ans pour faire une Puce PS2 fiable et digne de ce nom. Bien entendu sans tous nos problèmes juridiques on aurait pu faire cela bien plus vite.

Cinq puces pour la Xbox, une soixantaines de jeux en quelques jours, c'est énorme !

A l'heure actuelle il y a 2 alternatives pour XBOX. La notre et l'XTENDER, notre concurrent. Les autres puces dont on entend parler, ne sont en fait que des simples copies de ces deux puces, revendues sous d'autres noms. Si on compare cela à la PS2, où il y a peu près 20 solutions différentes, on est loin du compte, bien entendu nous n'en sommes qu'au balbutiement de la XBOX. L'engouement a commencé le jour des releases de RIOT et PROJECT X. La XBOX a été délaissée par les consommateurs, et tous les professionnels vous le diront, les ventes ont été jusqu'à présent CATASTROPHIQUES ! Si Microsoft avait continué sur cette lancée, on aurait donné très peu de l'avenir de la XBOX. Ce constat, nous le déplorons, est souvent le même dans la plupart des cas de figures. Nous sommes contactés, par des fabricants de lecteurs DVD, pour proposer des solutions de dézonnage, et pour reprendre leur propres mots: "Si ça n'est pas dézonné, on ne vend rien." Il est évident que sans nous ou d'autres, l'engouement autour de la Xbox n'aurait jamais été le même. Aujourd'hui les gens réagissent de la façon suivante : XBOX + PUCE = 380 euros, ça vaut le coup. Le calcul XBOX seule pour 299 personne n'en veut !

Craignez vous les foudres de Microsoft ?

Si nous les craignons ? Bien sûr ! Seulement comme je l'ai dit plus haut, nous ne savons pas faire grand chose d'autres. Maintenant il faut bien réaliser la situation et essayer de la comprendre avant de choisir son camp. Sommes nous bons ou mauvais ? Aux yeux des multinationales, nous sommes bons quand cela les arrange, notamment pour les modifications de lecteurs DVD, mais moins bon, pour le reste ! Nous ne cautionnons pas le piratage. On ne se voile pas la face pour autant, nous savons très bien qu'une grande partie des utilisateurs de nos produits vont en faire un mauvais usage. Sommes-nous responsable pour autant ? Peut être même moins que les vendeurs de graveurs ! Aujourd'hui on essaye de nous diaboliser, parce qu'il est plus simple de tirer sur un petit groupe que sur des millions d'individus.

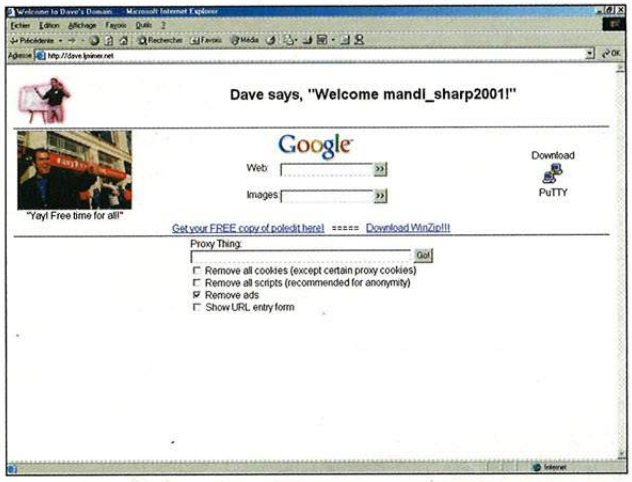
Et pour le GameCube ?

C'est en cours. Sortie d'ici un mois je pense. On ne peut pas en dire plus pour le moment !

EasyEveryThing a eu chaud !

Le réseau de cybercafés de EasyGroup a eu chaud, très chaud. Un pirate avait trouvé le moyen de devenir maître du système en pouvant modifier, effacer, ou créer des millions de comptes de part le monde. De quoi transformer, par exemple, cette chaîne de cyber cafés en zombi cybernétique.

Drôle de journée pour la société EasyEveryThing en ce début d'avril. Des gamins, ont eu accès, on ne sait par quelle magie, à une page d'un informaticien qui offrait la possibilité de pirater tous les cybercafés EasyEveryThing. Les gosses ont d'abord, semble-t-il, accédé à un serveur web appartenant à un certain Dave. Login et mot de passe en poche, le site offrait une série d'options sans grand intérêt. Moteur de recherche, liens, et une photo. Celle du patron de la société EasyGroup. Le PDG affiche un air jovial devant un de ses cybercafés EasyEveryThing avec sous la photo une légende : "Yay! Free time for all!". En cliquant sur ce document qui aurait pu sembler anodin, un logiciel nommé dave.exe se télécharge sur l'ordinateur des gamins. Un clic et un reboot plus tard, le tour est joué. Les voilà administrateurs de réseau Eayseverything...et de son nom de domaine. Panique à bord , nos gamins sont maîtres de la trentaine de cyber café de la société et cela sur toute la planète avec modification de comptes, proxy, ... Imaginez le méchant délire.



La ronde des mots de passe

Un traffic d'accès Internet s'est mis en place à Paris

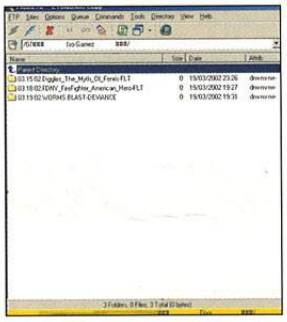
Vous souhaitez surfer gratuitement. Vds logins et mots de passe pour connexions illimitées et gratuites. Téléphonez au 0665xxxxxx". Voilà une étrange annonce passée dans le journal gratuit "Paris Paname" de cette fin mars. Des logins et mots de passe vendus comme ça, de main à la main. Nous avons voulu en savoir plus. Téléphone en main, nous prenons contact avec cet étrange vendeur. On nous propose un cd-rom contenant des centaines d'accès Internet illimités pour quasiment tous les acteurs du marché de la connexion au réseau. Le prix ? 150 euros, soit prêt de 1000 francs. Comment a-t-il eu ces mots de passe ? Mystère et boule de gomme. Il y a fort à parier que des bases de données ont été volées aux providers, mais aussi, par le social engineering. Une méthode utilisée par les pirates pour récupérer des informations privées à leurs victimes par simple utilisation de la ruse. AOL est l'un des premiers fournisseurs d'accès à voir ses clients continuellement attaqués de la sorte. Faux e-mails, faux sites, réclamant pour x raisons les logins et mots de passe. Le plus terrible et que cela fonctionne une fois sur deux.

Ma machine est un zombi

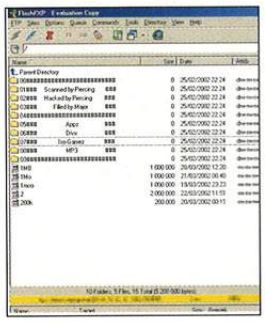
Pourquoi certains pirates tentent de posséder un maximum de mots de passe pour avoir accès à votre micro ? Dans cette catégorie de pirates, vos informations privées, le contenu de vos disques durs, ils s'en moquent un peu. Non, l'intérêt est ailleurs. Avoir la main sur votre ordinateur va leur permettre dans un futur proche ou non, de se servir de votre connexion comme un rebond, une passerelle entre lui et sa victime finale. Il peut utiliser des dizaines de rebonds de part le monde, rendant son délit quasi transparent et très difficile à remonter pour les forces de l'ordre. Un conseil, n'hésitez pas à demander à votre provider de changer votre mot de passe d'accès à Internet régulièrement !

Piratage de logiciels

Décembre 2001. Plusieurs centaines de policiers, douaniers et agents du FBI agissent au même moment dans une quinzaine de pays. Il est 6 heures du matin, l'opération Boucaniers vient d'être lancée. Cette opération vise l'un des plus important groupe de pirates de logiciels de la planète. ZATAZ Magazine a enquêté dans le milieu du warez.



Jeux cachés sur un ftp d'une entreprise. La société n'est même pas au courant



Un accès à un ftp pirate. Ici, un serveur piraté pour y laisser les copies de jeux, films, mp3, ...

Une liste des nouveautés warez du jour.

12 décembre 2001, 06 heures du matin

27 villes des Etats-Unis, quinze pays, dont l'Australie, la Grande-Bretagne, la Finlande, la Russie ou encore la Norvège font partie d'une des plus importantes actions contre un réseau de contrefacteurs de logiciels. Le groupe se nomme *DrinkorDie*, comprenez, boire ou mourir. Ce groupe, formé en Russie en 1993, est l'un des plus importants groupes de Warez Warrior de la planète informatique. Ils copient logiciels, films, bandes dessinées ou musiques. La police vient de mettre la main sur les principales têtes pensantes de ce réseau international de Warez. *DrinkorDie* est devenu l'un des plus importants groupes de copies de logiciels à partir de 1995. Il avait, par exemple, mis sur le réseau, 15 jours avant sa mise en boutique, le logiciel Windows 95 qui a fait la fortune de Microsoft.

Un peu d'histoire

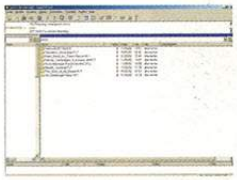
La contrefaçon de logiciel est nommée sur le réseau sous le sobriquet de Warez. Le warez correspond aux logiciels copiés. Il y a deux catégories de warez : Les jeux, Les "games" nommés gamez et les logiciels de types utilitaires, les applications, appelés appz. Le mot warez provient de la fusion du mot anglais marchandise "ware" et du pluriel underground qui utilise la lettre Z. Le Z ayant une connotation provocatrice. Il suffit de regarder certains groupes de rap trash, comme Sunz of man pour comprendre comme la lettre Z est devenue très "underground". Le mot warez serait apparu dans les années 20 puis réutilisé à la fin des années 80 pour parler des contrefaçons informatiques.

Il faut savoir que les warez ont toujours existé. L'un des premiers groupes à copier des logiciels, ça se passait sur ZX Spectrum, se nommait West Coast Crackers et nous sommes en 1987. Toutes les machines ont eu leur groupe de pirates. Sur Amstrad CPC avec des teams comme les TB crackers, Exocet, Xor, Two mag. Sur Atari avec les Réplicants ou encore Skidrow. Sur Amiga et aujourd'hui sur PC avec des groupes comme Fairlight, Razor 1911, PC Class, Paradigm, Divine, Paradox, DEViANCE, pour les plus connus. Certains officient dans ce milieu depuis plus de 15 ans. Les premiers piratages seront fortement favorisés par de petits boîtiers branchés directement sur les ordinateurs. A l'époque de l'Amstrad CPC, il existait déjà des extensions permettant de jouer avec n'importe quelle copie. Un gros boîtier qui se collait derrière le clavier, boite magique nommée la multiface. L'Atari a connu lui aussi son bout de plastique bourré d'électronique qui permettait aussi de ripper, d'enlever musiques et images d'un logiciel et cela d'une pression sur un bouton. Les plus anciens doivent se souvenir du Multiripper sur Atari ST.

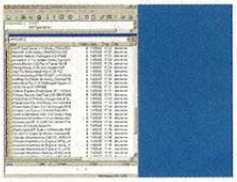
Warez or not warez

La contrefaçon sur Internet, vous avez dû vous en rendre compte en tapant ce mot dans un moteur de recherche de type Google, est énorme. Il existe de milliers de sites Internet proposant copies de jeux et autres utilitaires. Ils se divisent en groupes et sous groupes. De l'Elite au Lamer. La majorité de ces sites ne font que relayer des liens proposant de télécharger les contrefaçons. Très souvent les liens ne fonctionnent pas ou alors contiennent tout autre chose que la copie tant convoitée. Cela peut aller

Une cracktro de Paradox sur Playstation



Un accès pirate proposant des nouveautés contrefaites.



Accés à un ftp pirate proposant les Appz du jour.

Des sites web proposent des listes de centaines d'accès à des ftp pirates.

Certains sites fournissant des jeux pirates se protégent des autres sites sangsues.

du virus à la connection sur un serveur audiotel à 2 euros la minute. L'autre catégorie de ces sites, ceux des élites, proposent leurs propres réalisations. Mots de passe et protections contre le leech pour empêcher que d'autres sites viennent les piller. Le warez sur Internet peut donc être trouvé sur les sites web, et pourtant la vraie mine, la vraie caverne d'Ali baba ne se trouve pas là. Comme pour les films Divx, voir ZATAZ Magazine papier numéro 2, les vrais réseaux sont cachés bien plus profondément, souvent même dans des serveurs d'entreprises qui ne se doutent pas de ce qu'il peut se passer chez eux. Nous allons y revenir un peu plus tard.

Crack, patch, serial

Il faut savoir que les vrais groupes de pirates de logiciels, les Elites, utilisent peu, voire pas du tout le web. Ils vont plutôt passer par des moyens plus rapides et discrets comme les FTP. Le grand jeu étant de trouver des serveurs d'entreprises, par exemple, pour y laisser leurs butins. Seulement voilà, ici, les groupes prennent de plus en plus de risques. Ils piratent aussi les sites web afin d'y avoir un accès. La faille IIS, permettant avec un simple url trafiqué d'avoir accès aux disques durs d'un serveur non protégé, est du pain béni pour les amateurs de warez. Une fois un accès découvert, les groupes y déposent leurs réalisations, diffusent aux compte goutte l'adresse et disparaissent dans la nature sans laisser de trace. Pratiquement aucune entreprise ne prête attention à cette bande passante qui explose un jour puis revient à la normale 48 heures plus tard. Un espace de stockage à l'œil qui, en France, tombe sous la loi Godfrain, avec intrusion et maintient dans un système informatisé. Risque juridique doublé avec l'acte de contrefaçon.

Le monde du warez est comme vous l'avez vu découpé en petites communautés, divisées elles-mêmes en sous réseaux. Après avoir vu la diffusion de logiciels, nous allons voir les autres moyens de piratage mis en place. On commence par les cracks. Un crack est un petit logiciel de quelques kilos-octets qui aura pour but d'annuler une protection contenue dans le logiciel convoité. Il permettra, par exemple, de ne plus limiter un logiciel sur une durée, 30 jours par exemple, ou mettre en place toutes les fonctions, comme la sauvegarde qui a pu être désactivée par le fabriquant. Il suffit très souvent de cliquer sur le crack et le tour est joué. Il existe ensuite les serialz. Le serialz, comprenez le numéro de série, le mot de passe, sont de plusieurs sortes. Soit le groupe de pirate diffuse le mot de passe avec le logiciel, il ne reste plus qu'à l'utilisateur de rentrer le code dans la partie *Registration* du logiciel. Soit le groupe de pirates proposent un petit logiciel qui va générer lui même le bon mot de passe selon les critères mis en place par ceux qui auront tenté de protéger leur logiciel. L'un des outils les plus connu sur le web à ce sujet se nomme Oscar. Il propose des milliers de serialz pour quasiment tous les logiciels diffusés sur la planète

Le logiciel piraté est souvent décortiqué, vidé des parties considérées comme inutiles comme les vidéos ou les musique. Très souvent les meilleurs crackers débuguent les

Nul n'est censé ignorer la loi

En France, le Code de la propriété intellectuelle compte les logiciels parmi les "oeuvres de l'esprit" susceptibles d'être protégées, ainsi que le matériel de conception préparatoire (article L. 112-2, 13ème du Code de la propriété intellectuelle).

L'originalité du logiciel n'est pas contestable, nul n'est admis à le reproduire (article L. 122-4 du Code de la propriété intellectuelle) ni à l'installer, sans autorisation préalable du titulaire des droits d'auteur. La simple utilisation d'un logiciel piraté est donc susceptible de caractériser une contrefaçon. L'article L. 335-4 du Code de la propriété intellectuelle explique que les contrefacteurs risquent de deux ans d'emprisonnement et de plus de 152 400 Euros, soit un million de francs d'amende. Le Tribunal qui condamne un contrefacteur sur ce fondement peut également ordonner la fermeture totale ou partielle, définitive ou temporaire de "l'établissement ayant servi à commettre l'infraction ". Bref, des règles à ne pas prendre à la légère. Un exemple concret, l'équipe MJ 13, contrefacteur de logiciels existant depuis 1996 a été jugée par le Tribunal correctionnel de Paris qui a condamné ses deux têtes actives à 10 mois de prison avec sursis et 30 000 francs d'amende ainsi que 50 000 francs au titre de dommages et intérêts. Le second a été condamné à une peine de 4 mois de prison avec sursis et 4000 francs d'amende. Ne pensez pas qu'un avertissement sur votre site expliquant que la copie peut être gardée 24 heures vous protège. Sachez que ce genre d'avertissement n'est rien d'autre qu'une légende urbaine. Il est strictement interdit de mettre à disposition une quelconque copie.

Adobe traque le warez

Adobe a annoncé que sa nouvelle politique anti-piratage allait être radicale. Des dispositifs ont été placés dans les versions photoshop 6.1, ainsi que la version photoshop 7, qui doivent permettre de traquer les pirates de leurs logiciels. Il parait que ce système permet de collecter l'ensemble des numéros de séries piratés ainsi que les IP correspondantes. Adobe system Inc, aurait déjà un fichier de 250.000 adresses IP qui auraient été communiquées au FBI. Ca va être marrant de contrôler ce petit monde. Photoshop 7 étant un peu partout sur le réseau en version warez, il y a une paire d'agents du FBI qui ne vont pas beaucoup dormir ! Enfin, d'après le site web Présence PC, la nouvelle version du service de mise à jour de Windows Update serait capable de connaître le numéro de licence de votre Windows. Un outil qui doit permettre de contrer et éradiquer les versions pirates. Cette condition figure clairement sur les nouvelles conditions générales d'utilisation. Un autre exemple d'outil anti-pirate qui espionne aussi les honnêtes utilisateurs."

logiciels afin de les rendre 100 % fiables. Un sacré pied de nez aux éditeurs. Dans les années 90, une société de jeux vidéo, Cobra Soft, avait ainsi inséré dans le code de programmation de ses jeux, un message dédié aux pirates : "Rejoignez-nous, ne jouez plus aux pirates". La société avait laissé son adresse pour d'éventuelle mise en relation.

Réseaux pirates

Les réseaux de pirates de logiciels sont très structurés. Il n'existe plus aujourd'hui de cracker qui dans son coin va trouver le logiciel à déplomber, le transformer, le diffuser. Les structures de ces groupes sont nettement plus impressionnantes et organisées. On y trouve d'abord le *supplyer*. Il est celui qui va fournir la nouveauté à déplomber. "Pas mal de nos réalisations proviennent directement de certains salariés d'éditeurs de jeux" dixit un des pirates que nous avons pu rencontrer sur IRC. La légende veut que le premier *Supplyer* fut la poubelle de la société de jeux vidéo LORICIELS. Chaque soir des pirates la visitait pour récupérer les disquettes jetées et ainsi reconstituer les jeux que préparaient dans le plus grand secret cette société aujourd'hui disparue. Dans cette chaîne warez intervient ensuite le *cracker*, celui qui va casser, retirer la protection. Le *cracker* est aussi appelé *déplombeur*. Une fois le logiciel déprotégé, la team va dans la majorité des cas y placer une introduction lors du lancement du jeu. Une forme de carte de visite qui est très souvent agrémentée d'options pour faciliter la vie du joueur. On appelle cela un *traîner*. Vie, énergie, armes infinies font partie des options les plus demandées dans un traîner. Une fois le package du groupe prêt à être diffusé, les *swappers*, ceux qui diffusent,

ZATAZ magazine vous révéle comment certains éditeurs de logiciels piégent les pirates.

Nous allons prendre ici l'exemple de l'une des protections anti-cracking de chez Minnetonka Software. Ce logiciel de plusieurs milliers de dollars vaut bien une protection par comme les autres.

Surcode DVD DTS Pro, le produit de Minnetonka Software intègre un système de protection qui laisse songeur. Loin des habituels spyware, qui se contentent de faire passer un certain nombre d'informations aux sociétés de Marketing ou, à la limite, le numéro de licence d'un logiciel à la maison mère, Minnetonka innove. Il ne s'agit plus de tracer d'éventuelles copies pirate d'un logiciel donné mais d'agir en amont, en traçant les pirates au moment ou ils commencent à cracker le soft. Le principe est relativement simple.

Cette société a protégé une partie de son logiciel avec un code binaire piégé. Le binaire intègre une instruction qui est régulièrement utilisée. Le temps d'exécution de celle-ci est systématiquement vérifié. Si la durée d'exécution est anormalement longue, une alerte est générée: on considère que quelqu'un est en train de débuguer le binaire. A partir de ce moment une alerte par courrier électronique est auto-générée. Le système d'alerte est basé sur le mail. Mais plutôt que d'utiliser la messagerie du cracker, qui peut être très différente d'une machine à l'autre, Surcode DVD DTS Pro va générer son propre message, en se connectant sur le serveur mail (SMTP) de la société éditrice (cf. Schéma). Le mail qui est construit ressemble à cela (dans cette exemple, on considère que l'IP du cracker est 100.100.100.100 et se nomme machine.cracker.com):

Return-Path: <100.100.100.100>
Received: from machine.cracker.com (machine.cracker.com [100.100.100.100]) by perseus.minnetonkasoftware.com (8.9.3/8.9.3) with SMTP id FCE01234 for <info@minnetonkaaudio.com>; Wed, 1 May 2002 08:43:18 -0600
Date: Wed, 1 May 2002 08:43:21 -0600
From: 100.100.100.100@minnetonkasoftware.com
Message-Id: <200205010843.FCE01234@perseus.minnetonkasoftware.com>
X-Authentication-Warning: perseus.minnetonkasoftware.com: machine.cracker.com [100.100.100.100] didn't use HELO protocol
Status:
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000
X-UIDL: 123ab45c000067d8

abc machine 100.100.100.100 1234 surcodedvd.exe

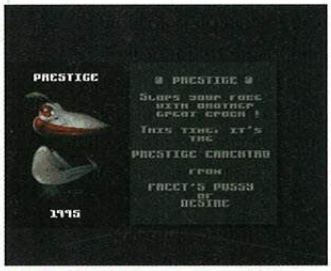
Une fois l'alerte lancée, une gestion de l'incident est sous-traitée par une société spécialisée. En cas d'incident lié à une tentative de cracking en Europe, c'est la société NetResult Ltd, de Londres, qui entre en contact avec les responsables sécurité du réseau depuis lequel la tentative a été enregistrée. Spécialisée dans les droits digitaux et la fraude informatique, elle est chargée de donner une éventuelle suite juridique au problème. Une recherche "netresult infringement" dans Google vous donnera la mesure de leur efficacité. Zataz Magazine le dit depuis toujours : Pirater des logiciels c'est mal. Mais aujourd'hui on vous prouve que, avec ce genre de protection, ça peut FAIRE mal. Surtout si votre employeur reçoit un courrier de NetResult Ltd.

Photo : Dreamworks

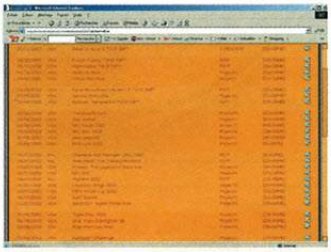
entrent en action. Le but du *swapper*, diffuser les warez fraîchement déplombés, le plus rapidement et efficacement possible. Il est souvent appelé aujourd'hui "Swapper-scanner" car il va chercher les endroits ou les warez pourront être distribués. Depuis plusieurs mois, un grand nombre d'entre eux scannent les sites web de la planète à la recherche de la faille IIS Windows NT. La faille unicode découverte permet l'accès à une partie du disque dur du site convoité, permettant ainsi au *swapper* de laisser ses colis en quasi transparence. " Certains swappers prennent de plus en plus de risque pour diffuser les news. Ils pénètrent des serveurs web et un jour ça va mal finir." dixit un membre d'un de ces groupes de pirates de logiciels que nous avons rencontré durant notre enquête.

Le site de l'une des puces pour Xbox
www.xboxmods.co.uk
Vidéo du groupe ProjectX
playstationmods.com/xbox/neox.wmv
Le site de Minnetonka audio
www.minnetonkaaudio.com/Products_3.htm
Le site du groupe Xtender
www.xtender.info
La loi française et les contrefacteurs
www.legalis.net/legalnet/cpilog.htm

Une cracktro du groupe Fairlight. Ce groupe à 15 ans.



Une cracktro du groupe Razor 1911


La liste des jeux Xbox piratés.

Les risques et enjeux

Le marché des jeux vidéo a avoisiné les 16 milliards d'euros en 2001. Le manque à gagner, dû au piratage, a été estimé à près de 2 milliards d'euros d'après l'étude effectuée par le EITO. Il faut savoir que prêt de 40 % des CD vierges vendus seraient utilisés pour la copie de logiciel. Les éditeurs ont depuis le début tenté d'endiguer le problème, sans grand résultat. Lors de notre enquête nous avons même découvert que beaucoup de sources des réseaux warez étaient directement liées à des salariés de sociétés de Jeux Vidéo. Dommage que les services de presse de ces sociétés n'ont pas souhaité nous répondre à ce sujet... Ils sont plus efficaces à nourrir le journaliste de communiqué de presse et de petits pains surprises lors des conférences de presse qu'à répondre clairement à ce problème qui les touche. La rumeur chez certains groupes warez fait état même d'une certaine connivence entre eux et certains éditeurs. Certains de ces éditeurs dont nous n'avons pas eu le nom n'hésiteraient pas à pousser quelques copies dans la nature. "Certaines sociétés ont aussi la main légère quand il s'agit d'un produit d'un concurrent" dixit Max, membre d'un groupe de fournisseurs de Warez . Alors à qui profite vraiment le crime ?

Protections anti-copies

Il existe des dizaines d'autres formes de protection. Les plus farfelues ont été, par exemple, l'utilisation d'un virus dans le jeu G360 de Sega sur Amiga. Les utilisateurs de la contrefaçon de ce jeu d'avion se voyaient gratifiés d'un beau message d'erreur moqueur quelques minutes après le lancement d'une partie. Dans un autre style, le jeu GOD, toujours sur Amiga, des Bitmap Brothers, devenait fou en pleine partie. Impossible de jouer tant les ennemis tombaient du ciel. Plus récemment, Codemasters a réutilisé cette protection anti-copie dans son jeu Opération Flashpoint. Cette protection, qu'ils ont nommée F.A.D.E. altère le jeu à un point où la copie de ce dernier devient injouable. Des anti-copies qui peuvent empêcher aussi les originaux de fonctionner correctement.

Le système Anti-copie de Championship manager 3 d'Eidos était tellement mal fichu qu'il empêchait de jouer sur certains ordinateurs.

Les crackeurs auront dans tous les cas réussi, à chaque fois, à passer ces protections. Le groupe DEViANCE ira jusqu'à noter dans son piratage de Flashpoint ceci : "Additional note: while we tested we found no trace of the 'fabulous' 'FADE protection' - so we can only assume for now that the press releases about it were just the usual company bullshit". En gros comprenez que ce groupe de pirates de logiciels n'a pas trouvé trace du F.A.D.E. dans le jeu, annonçant même un effet marketing de Codemaster. D'autres protections comme le "CD-Cops", qui ajoute à l'exécutable du Cd Original une protection mesurant la durée en minute et seconde d'un CDROM ou encore "DiscGuard" qui ajoute une signature. Une protection tellement efficace qu'elle empêchait, par exemple, le jeu original Collin Mac Rae de fonctionner. A Codemaster de fournir des patchs pour annuler cette protection ! Les magazines traitant de jeux vidéo ne sont pas non plus à l'abri. Les sociétés éditrices fabriquent aujourd'hui des versions dédiées aux testeurs des magazines en y incrustant le logo de leur revue pour empêcher les copies. Pourquoi tant de méfiance ? Les exemples de logiciels fournis à la presse et qui ont fini dans les poches des groupes de warez pullulent. L'un des plus marquant est l'affaire qui aura touché le magazine Amiga Concept, disparu aujourd'hui. Ce journal fut condamné après qu'un de ses pigistes eut vendu le jeu Blob de Psynopsis à un groupe de pirates de logiciels.

Protéger tous vos CD contre la copie

Alors que l'on nous parle un peu partout de la facilité à casser les protections de logiciels, nous allons vous montrer qu'il n'est pas si compliqué de protéger ses propres créations sur CDROM. Attention, notre méthode n'est pas infaillible, mais suffisamment sûre pour contrer les fous du graveur.

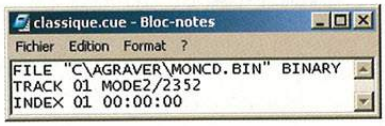
Toc, Toc, Toc

La TOC illégale, comprenez le blocage de la table des matières, est la protection que nous vous proposons de découvrir. Elle fait partie de ces systèmes de protection qui exploitent les incohérences tolérées dans la gravure de CD. Elle empêche également toute copie physique d'un CD et peut s'appliquer aussi bien à la protection de vos CD-Rom qu'à celle de vos CD-Audio. Le plus souvent, cette protection empêche seulement la copie physique du CD sans pour autant faire obstacle à certain logiciel de gravure comme CloneCD... De plus, le matériel a tellement évolué que seulement quelques graveusr et lecteurs haut de gamme sont capables de passer outre cette protection. Résultat : le CD devient copiable. Mais encore faut-il avoir le bon matériel et savoir se servir correctement du logiciel de gravure. La TOC illégale est aujourd'hui à la base d'un grand nombre de protections. Pour mieux la comprendre, je vous propose de la mettre d'abord en pratique de manière manuelle, puis de manière automatique par le biais des logiciels qui l'exploitent tacitement.

Protection maison

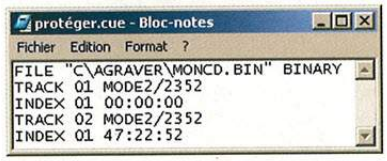
Pour intégrer une TOC illégale à tous vos CD, il suffit que vous ayez à votre disposition le logiciel de gravure CDR-Win ainsi que Notepad, l'éditeur de texte fourni en standard dans Windows.

Etape 1 : Création de l'image-disque.



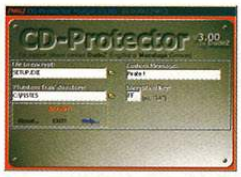
La toute première chose à faire est de créer l'image-disque du CD à protéger. Pour cela, nous allons utiliser CD-R Win. Au final, les informations utiles à la gravure de notre CD seront contenues dans un fichier texte appelé Cue sheet.
Celui-ci contiendra l'ordre des pistes à graver, leurs natures, ainsi que leurs positionnements (optionnel). Ce fichier est en fait une sorte de table des matières, ou Table Of Content (TOC) en anglais, qui se retrouve également dans la structure du CD. C'est au niveau de ce fichier texte que nous allons devoir intervenir pour mettre en place notre protection.
Bien évidemment, celui-ci pourra changer en fonction des caractéristiques du CD à protéger (Wave à la place de Binary, Mode 1/2352 ou Audio à la place de Mode2/2352, ...)

Etape 2 : Intégration de la TOC illégale.



Pour mettre en place la TOC illégale, nous allons d'abord créer une seconde piste virtuelle d'une durée de deux secondes. Pourquoi deux secondes ? Tout simplement parce qu'il est stipulé dans le Yellow Book et dans le Red Book, les deux livres techniques définissant les caractéristiques des CD-Rom et des CD-Audio, qu'une piste doit obligatoirement

avoir une durée minimale de 4s pour être conforme avec la norme CD. Bizarrement, certain logiciel de gravure (Ndr : comme CD-R Win) n'effectue aucune vérification quant à la durée des pistes qui devront être gravées... Une aubaine pour la protection de notre CD. En sachant cela, il nous suffit de retirer deux secondes (ou trois) à la durée totale des données stockées sur notre CD à protéger pour mettre en place notre TOC illégale. Pour cela, nous devons impérativement l'indiquer dans la Cue sheet. Faites d'abord Record Disc / Load Cuesheet afin de recharger la Cue sheet créée précédemment. CDR-Win va vous indiquer le Total Disc Time du CD (la durée totale du disque). Supposant que dans notre cas, il fasse 47 : 24 : 52. Enlevons ensuite deux secondes à cette durée



(soit 47 : 22 : 52) et entrons cette nouvelle information après avoir créer notre seconde piste virtuelle. Voilà ! A ce stade, il ne vous reste plus qu'à vérifier que CD-R Win a bien pris en compte vos modifications en faisant Record Disc / Disc Layout ou celui-ci vous affichera la nouvelle piste ainsi que la durée réelle du CD à savoir 47 : 24 : 52. Il ne vous reste plus qu'à graver votre CD... Le principe de la TOC illégale étant maintenant acquis, il ne nous reste plus qu'à voir les outils qui l'exploitent intelligemment.

Protection automatique

Il existe actuellement quelques outils freewares qui vous permettront d'automatiser la protection de vos propres productions. Ils suivent le même schéma de principe que celui de la TOC illégale en apportant cependant quelques innovations. Pour la circonstance, j'en ai choisi deux qui me semblent les plus aboutis : CD Protector et CloneAudio Protector.

CD Protector

CD-Protector est un logiciel freeware qui s'adresse à tous ceux qui souhaitent développer une application sur CD-Rom. Il permet le cryptage de l'exécutable principal du programme (par exemple, le Setup de l'installation) tout en empêchant la copie physique du CD par l'utilisa-

tion d'une TOC illégale plus que complexe. La protection se faisant en amont, la gravure devra par contre se faire sous Nero, bien que cela ne soit pas rédhibitoire.

Clone Audio Protector

Clone Audio Protector est logiciel freeware qui utilise deux techniques très différentes pour protéger les CD-Audio. La protection SYS est une variante plus complexe de la TOC illégale. Quant à la protection Cactus Data Shield, elle se base sur certains travaux de la société israélienne MidBar Technologies. Les CD qui en résulteront seront non seulement incopiables mais leurs lectures sur les ordinateurs, les consoles de jeux ou encore les lecteurs de MP3 sera totalement impossible. Pour qu'une protection soit efficace, il faut qu'elle sache contrer à la fois la copie unitaire des fichiers ainsi que la copie physique du CD. Deux tâches bien distinctes qui nécessitent une double approche dans la protection de votre CD. Ce n'est pas le cas de cas de la protection manuelle, qui n'était là qu'à des fin de théorie, alors que l'utilisation des logiciels présentés dans la protection automatique l'intègre en standard... Tirez-en vos conclusions !

GLOSSAIRE

Total Disc Time du CD : La durée totale du disque.

TOC : Ce fichier est en fait une sorte de table des matières, ou Table Of Content (TOC) en anglais, qui se retrouve également dans la structure du CD.

A lire

Pour en savoir plus deux livres indispensables de Christophe Fantoni auteur de "Comment créer vos propres DVD" et de "L'Enregistrement numérique sur CD et DVD" édités aux éditions Dixit (www.dixit.fr)

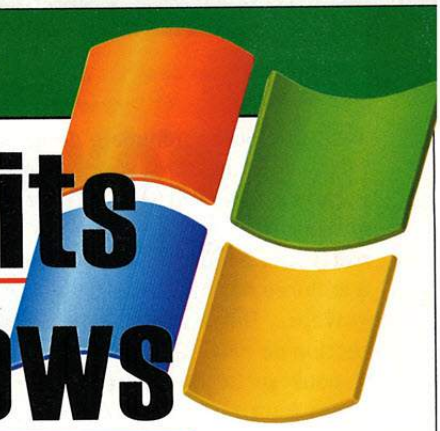
Logiciels

Clone-cd : http://elby.ch/english/products/clone_cd/index.html
CDr-Win : www.goldenhawk.com/download.htm
Clone audio protector :
http://mag.zataz.comCd-Protector :
http://mag.zataz.com

Ne manquez pas notre newsletter !

ZATAZ Magazine vous propose chaque semaine une news letter d'actualité et d'information technique. Pour 50 euros, recevez chez vous, dans votre boite e-mail, au format PDF, l'informations en exclusivité. En bonus, vous recevrez gratuitement ZATAZ Magazine papier chez vous pendant un an. Pour en savoir plus http://www.zataz.com/zataz/mail2.htm

Maîtriser les petits secrets de Windows



Windows pourrait largement remporter la palme d'or de l'OS (Operating ystem) le moins sécurisé. Voici un petit récapitulatif sur toutes les astuces intéressantes et utiles. Dernière chose avant de commencer, personne n'est à l'abri d'une erreur, alors pensez, avant de suivre nos conseils, de faire une copie sauvegarde de vos fichiers... au cas où !

Surveillance utilisateur

Dans un profil multi-utilisateurs, afin d'empêcher que le nom du dernier user apparaisse, allez dans Hkey_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Winlogon.
Créer une DWORD : Don'tDisplaylastUserName et affectez-lui la valeur 1. Votre nom d'utilisateur n'apparaîtra plus.

Bloquer l'accès DOS d'un système

Même si l'on utilise un mot de passe sous Windows au démarrage ou alors avec certains logiciels bloquant le système avant le démarrage de Windows, n'importe qui peut passer en Mode Sans Echec (par la touche F8 ou Ctrl). Il est possible de bloquer, non cet accès, mais le menu qui y apparaît. Tout réside dans le fichier MsDos.sys. Ouvrez ce fichier avec le Notepad (via Exécuter) et ajoutez-y ces lignes :
bootmulti=0
bootmenu=0
bootkeys=0
Désormais, le menu est hors service.

Mouchards Windows

Dans ZATAZ Magazine numéro un nous vous relations quelques techniques pour annuler certains programmes indiscrets de Windows, du moins les plus connus. Aujourd'hui nous allons traiter d'une autre séries de mouchards nettement moins classiques et qui n'ont jamais été traité, à notre connaissance, les "applogs".

Repérez le répertoire C:\Windows\Applog et \Applog.ind. Chaque fichier du dossier est une indication sur les programmes qui ont été ouverts. Ils ont été créés à l'heure de votre manipulation donc on peut savoir ce que vous avez fait et quand, juste en regardant leurs dates de créations dans les Propriétés de chaque fichier. Il est possible de supprimer cela de manière automatique à l'aide d'un fichier VBS. Appelez-le "AntiApplog.vbs", copiez-le dans Menu démarrer\Démarrage de votre dossier Windows et écrivez ceci à l'intérieur :

```
"
Dim fso
set fso =
CreateObject("Scripting.FileSystemObject")
fso.DeleteFolder("c:\Windows\Applog")
"
```

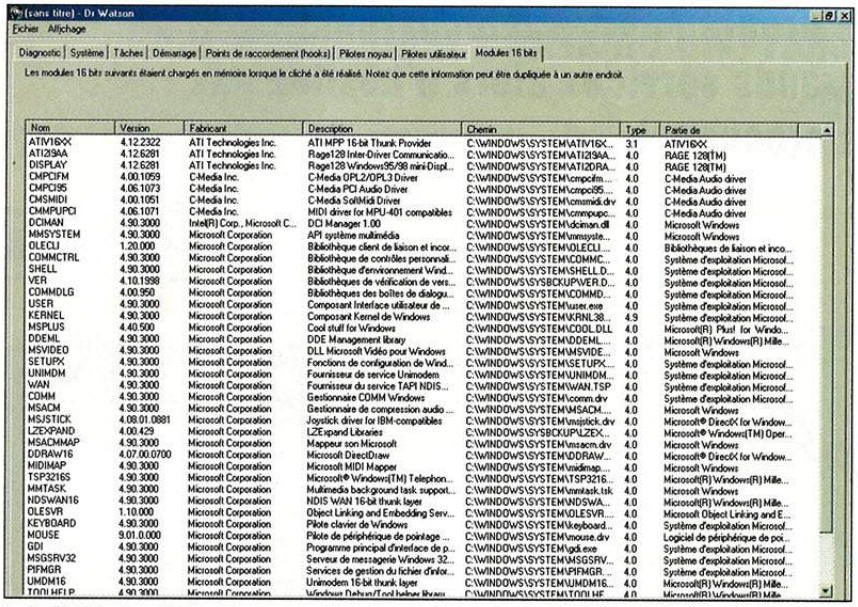
ShellIconeCache

Le fichier que nous allons étudier est une application cachée. Vous allez le trouver à cette adresse : C:\Windows\ShellIconeCache. Il répertorie exhaustivement tous les éléments démarrés depuis plusieurs semaines. C'est un fichier caché.

Pour le supprimer, il faut faire une manipulation préalable à restaurer immédiatement après. Allez dans le Panneau de configuration dans Système, utilisez notre raccourci Windows+Pause, sur l'onglet Performances. Cliquez sur le bouton "Mémoire virtuelle" et cochez la case "Me permettre de spécifier mes propres paramètres de mémoire virtuelle" et cochez la case "Désactivez la mémoire virtuelle". Notez avant d'agir les paramètres actuels de votre mémoire virtuelle existante. Ignorez le message d'avertissement et de reboot et virez les deux fichiers concernés. Puis rétablissez la mémoire virtuelle. Pour les fichiers Applog, ces derniers se créent automatique et vu la taille qu'ils prennent nous allons automatiser leurs destructions via un fichier en VBS. Pour cela, créez un fichier d'extension ".vbs" et inscrivez dedans :

```
"
Dim fso
Set fso =
CreateObject("Scripting.FileSystemObject")
fso.DeleteFolder ("c:\windows\Applog")
"
```

Il suffit que vous copiez ce fichier dans c:\Windows\Menu Démarrer\Démarrage pour qu'à chaque démarrage le dossier disparaisse et toutes vos traces avec.



Le logiciel Docteur Watson permet de rendre plus performant votre micro...A user sans modération !

Win386

Le fichier suivant se trouve à l'adresse suivante, C:\Windows\Win386.swp ou *.swp. Ici nous allons traiter d'un fichier d'échange Windows qui contient des bribes de fichiers textes surtout et beaucoup d'autres informations sur la configuration de votre PC.

Frères jumeaux

Si vous avez deux fichiers avec le même nom et les mêmes propriétés, il existe une commande Windows pour les comparer afin de pouvoir constater si ce sont des doublons ou non. Allez dans Exécutez et tapez: fc nomfichier1.abc nomdufichier2.def. abc et def sont les extensions des fichiers respectifs à contrôler. Une fenêtre DOS vous informera si les fichiers sont identiques ou non, auquel cas elle vous indiquera les différences constatées.

Supprimer "déconnexion" du menu démarrer

Allez dans Regedit, et recherchez la clé HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Vous allez ensuite créer une nouvelle valeur binaire "NoLogOff". Affectez-lui la valeur 01 00 00 00.

Soignez votre base de registre

Voilà une astuce qui va vous plaire. Redémarrez votre PC en mode MS-DOS et taper SCANREG /FIX pour reconstruire la base de registre afin d'optimiser ses performances.

Elémentaire mon cher Watson

Saviez-vous que Windows cache en son sein de petits programmes bien sympathiques. Prenons par exemple le logiciel Docteur Watson. Il se trouve dans le répertoire Windows au nom "Drwatson.exe". Votre ordinateur est lent au démarrage. Illico presto vous faites Ctrl + Alt + Suppr. Dr Watson va vous dire qui a une fâcheuse tendance à être bouffeur de mémoire et des ressources de votre ordinateur. Démarrez donc ce cher Dr Watson, il va apparaître alors dans le Systray, la barre où se trouve l'heure, dans la barre des tâches. Exécutez-le et il vous dira s'il y a quelque chose d'anormal dans le comportement de votre PC. Si tout baigne, allez dans Affichage et sélectionnez Affichage Avancé. En plus d'être relativement complet, différents onglets vous renseignent sur les ressources mémoire, les fichiers pilotes... Allez dans démarrage, et là s'affiche une liste exhaustive de tout ce qui est lancé au démarrage de Windows, en vous indiquant si cela se fait par le registre où si ce démarrage peut être configuré dans le logiciel lui-même. Bref, un vrai espion à votre disposition.

Propriétés système d'une machine, il existe un raccourci tout simple : appuyez simultanément sur les touches WINDOWS + PAUSE de votre clavier.

J'ai la mémoire qui flanche...

Voici une astuce à faire pour optimiser les performances d'accès mémoire de votre PC. Par le Panneau de Configuration\Système , dans l'onglet Performances, au bouton Mémoire virtuelle, vous pouvez "bouffer" littéralement de la mémoire en réglant manuellement (min=0 et max=1) la taille qui délimite en fait la taille maximale du fichier d'échange Windows et qui est indispensable pour que Windows dispose suffisamment de mémoire pour accéder aux différents programmes du disque. Il est également possible d'augmenter, ou tout aussi bien de diminuer, la taille du cache des disque-durs. Ouvrez le fichier system.ini et modifier, ou ajouter, ces lignes:

[VCACHE]
MinFileCache=65536
MaxFileCache=131072

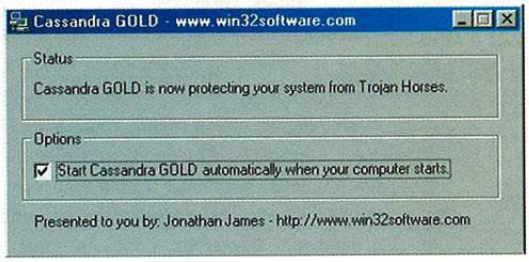
Bien sûr, vous pouvez modifier ces valeurs à souhait. Juste un petit truc bien utile : pour afficher les

Appz!

Voici notre sélection de programmes à télécharger. Tous vont rendront de grands services alors n'hésitez pas une seconde à vous les procurer !

Anti-espion

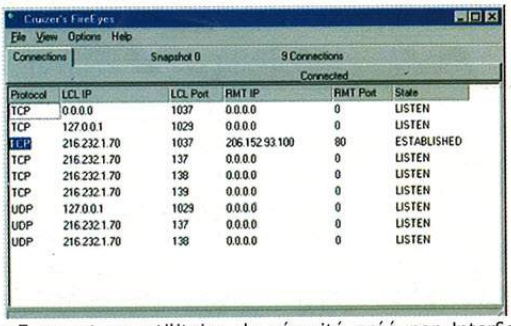
Nom : Cassandra GOLD Langage : FR Poids : 0,01 mo License : Freeware



Cassandra GOLD vous permet de protéger votre ordinateur contre de nombreux Trojan Horses et Backdoors. En mythologie grecque, Cassandra était la fille du roi Trojan et l'auteur de cet outil, Jonathan James, s'est inspiré de cette histoire pour créer un logiciel qui va vous permettre d'éliminer les chevaux de Troie suivants : BackOrifice 1.20; BladeRunner; COMA; Deep Throat 1.0, 2.0, and 3.0; GateCrasher 1.2; GirlFriend 1.35 (Ancien et nouveau); HACK99; Hack-a-Tack; Masters Paradise 9.7; Millenium; NetBus 1.6, 1.7, 2.0, et 2.01; NetSphere; NetSpy 2.0; OpC BO 2.0; Spying King; SubSeven 1.5; Telecommando; WEB EX 1.2; et WinCrash 1.03.

Fermer la porte aux intrus

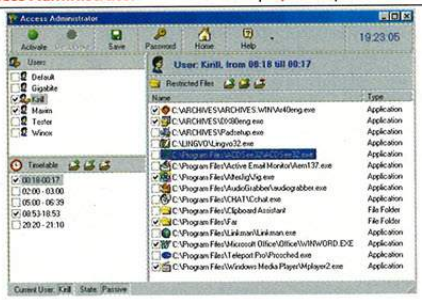
Nom : FireEyes // US | 0,41 mo | Freeware



FireEyes est un utilitaire de sécurité créé par InterSoft Software qui a pour but de surveiller toutes les connexions de votre PC. Le logiciel vous alertera si un pirate souhaite s'inviter chez vous. Il vous suffit de définir les ports que vous souhaitez contrôler et l'adresse à contacter en cas de tentative de visite.

Contrôler l'accès à vos fichiers

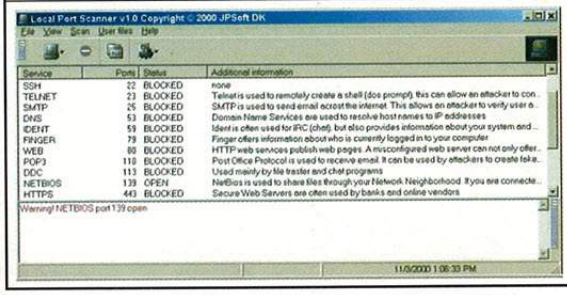
Nom : Access Administrator // FR | 0,8 mo | Freeware



La version 2.2 d'Access Administrator Pro va vous permettre de contrôler l'accès aux fichiers et dossiers situés dans votre ordinateur. L'outil est très utile car il va vous permettre de refuser l'accès à certains fichiers et dossiers ou de les dissimuler afin qu'ils ne soient pas vus ou recherchés. Vous pouvez même donner l'autorisation d'utilisation certains dossiers et logiciels durant des heures que vous aurez définis.

Portes ouvertes

Nom : Local Port Scanner Langage : US Poids : 0,50 mo License : Freeware



Local Port Scanner version 1.0 est un petit logiciel écrit par la société Danoise JPSoft qui va examiner les ports de communication de votre ordinateur. Des entrées qui pourraient servir à vous espionner, par exemple, via l'utilisation d'un cheval de Troie. Le programme peut détecter les ports le plus généralement utilisés par les intrus et les Trojan, il comporte cinq modes de balayage: TCP, rapide, Trojan, Stealth, et défini par l'utilisateur.

Pour télécharger ces logiciels, rendez vous à l'adresse
http://mag.zataz.com

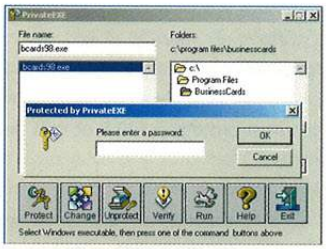
Chasseur d'espions

Nom : Trojans First Kit Langage : FR Poids : 0,1 mo License : Français

Trojans First Aid Kit est un outil qui va vous permettre de traquer et éradiquer pas moins de 140 troyens. De quoi voir venir quasiment n'importe quel neuneu du web en mal d'espionnage. Le programme peut également trouver de nouveaux Trojans inconnus en utilisant des méthodes de recherche, et vous fournit plusieurs outils pour les détecter automatiquement. Ce logiciel a été écrit par Snake Byte de la team allemande, Krypto Crew.

Protéger vos programmes

Nom : PrivateEXE // FR | 0,15 mo | Freeware



Voilà un logiciel qui va intéresser un grand nombre d'entre vous. Private EXE est un logiciel qui vous permet de mettre des accès par mots de passe aux exécutables de Windows. Il modifie les fichiers exécutables afin qu'à chaque lancement de ce dernier un mot de passe soit demandé pour en contrôler son accès.

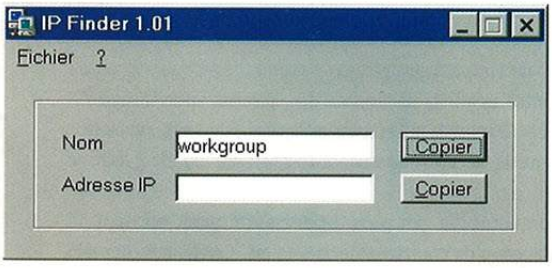
Surf pour les gosses

Nom : Amiweb // Fr | 4 mo | Freeware

Ce logiciel est un navigateur destiné à la famille et aux enfants. Yan Bourgeois, son auteur, offre plusieurs outils personnalisables en offrant ce qu'il y a de mieux en matière de jeux et de sites éducatifs pour les enfants, afin qu'ils puissent eux aussi profiter d'Internet comme leurs parents. Même si l'idée est très intéressante, on ne laisse jamais surfer un enfant seul sans être accompagné par un adulte.

Qui suis je ?

Nom : IP Finder Langage : Fr Poids : 0,01 mo License : Freeware



Vous êtes très nombreux à nous demander comment faire pour connaître l'IP qui vous a été allouée lors de votre connexion à Internet. IP Finder est une petite application de Sébastien Coutaz qui va vous permettre de connaître votre adresse IP et votre nom de machine lorsque vous êtes connecté sur le réseau. Cette application demande que soit installé sur votre machine le VB Runtime Files.

Interview

Brazil Hacker Sabotage

Au brésil il y a la plage, le soleil, le pain de sucre. Il y a aussi la plus importante, et active, communauté de défaceurs de pages web. Parmi les leaders des pirates de ce pays, l'équipe Brazil Hackers Sabotage : plus de 1500 sites modifiés en un an, comme par exemple : cineinfo.fr, recherche.mesfinances.fr, yamaha.fr, wcati.ac-poitiers.fr, ou encore Alcatel, Mac Do, Opel, Nokia, ... Nous avons souhaité en savoir plus sur cette équipe, leurs motivations. Interview avec SilentStorm du BHS.

Qu'est ce que le BHS ?

Le Brazil Hackers Sabotage (BHS) est un groupe fondé en mars 2001. Notre team est composée par trois jeunes Brésiliens, JShalom, SilentStorm et TuK. Notre centre d'intérêt principal est : la modification de page web et l'étude de technique et code pour créer des nouvelles méthodes d'attaque.

Vous êtes le second groupe le plus actif du web, pourquoi ?

L'objectif de notre groupe, depuis sa fondation, est de gagner le défi d'être le groupe de 'defacer' le plus important du monde. Aujourd'hui, BHS est en seconde position, et nous serons bientôt les premiers.

Il y a beaucoup de groupes de pirates informatiques au Brésil, pourquoi ?

Beaucoup de gens sont intéressés par la sécurité du web et cela implique aussi les attaques. La majorité sont des jeunes gens, de 15 à 25 ans, recherchant la connaissance et souhaitant s'amuser.

Qu'est ce qui vous plait dans le piratage ?

Les attaques nous donnent deux choses essentielles : connaissance et amusement. La possibilité d'avoir les deux en même temps rend cette " activité " intéressante.

Qu'est ce que vous aimez sur le Web ?

L'Internet est l'outil de communication le plus puissant jamais fait. C'est une très bonne source d'information et de connaissance, pas juste pour nous, mais pour tous, bien qu'il soit difficile de trouver de bons sites avec des informations utiles.

Vous n'avez pas peur de la police ?

Nos activités sont illégales, nous le savons, mais nous n'avons pas peur de la police, ou des autres autorités. Je crois qu'ils sont plus occupés par les enlèvements, les viols, les braquages, le terrorisme et d'autres choses biens réelles. Pour eux c'est de la merde et de la perte de temps que de vouloir arrêter les gens qui cassent la sécurité d'un site web. Je crois qu'ils ont des choses plus importantes à gérer et à s'occuper.

Quels sont les choses les plus étranges que vous ayez pu voir sur un serveur web ?

Rien de très étrange. Les serveurs sont essentiellement les mêmes. Il y a quelques situations drôles, bien sûr, comme l'attaque d'un serveur où l'administrateur s'y trouve en même temps que nous. Là, c'est très, très drôle.

Quels sont les attaques les plus difficiles ?

Je crois que les attaques les plus difficiles sont à l'encontre des serveurs sous OpenBSD. Difficile à trouver et il n'y a pas beaucoup de vulnérabilités à exploiter. Mais rien n'est protégé à 100 % et cela peut changer dans l'avenir.

Les attaques les plus simples ?

Difficile à dire, parce nous utilisons aussi des outils d'attaques fait maison, permettant ainsi des intrusions plus faciles. Aujourd'hui nous avons de très bonnes méthodes d'attaque contre Linux, Solaris et AIX.

Vous pensez arrêter le defacement un jour ?

Nous n'y pensons pas encore. Je crois que nous ne nous arrêterons jamais. Si nous arrêtons le defacement ça sera pour bosser dans des sociétés de sécurité, ou quelque chose dans le genre. C'est ce que nous aimons faire.

Qu'est ce qu'une bonne protection sur Internet ?

Aujourd'hui rien ne peut être protégé à 100 %. Protection aujourd'hui ne le sera plus demain.

Que pensez-vous de l'impact des pirates informatiques ?

Difficile de connaître le véritable impact des "pirates informatiques" dans le monde. Le fait est que les pirates informatiques contrôlent Internet et risquent de le contrôler encore longtemps.

Avez-vous été contactés par des gens "bizarres" : Armée, escroc ?

Nous recevons beaucoup de courriers électroniques. Certains de ces e-mails sont des menaces. Je ne crois pas que les autorités nous menaceraient via un courrier électronique, ça serait vraiment pathétique.

Foreign Threat
Deceptive Duo

Ils se nomment Deceptive Duo, deux américains qui ont décidé de lancer une mission, nommée : "Foreign Threat". Leur but, montrer que ce que raconte le gouvernement US est totalement ment au sujet de la sécurité informatique de l'Oncle Sam. "Ils ne savent pas se protéger, et donc, ne savent pas nous protéger". ZATAZ Magazine vous propose en exclusivité l'interview de ces deux étranges personnages.

Qui est le Deceptive Duo ?
Nous sommes deux pirates informatiques dont la mission est de démontrer que la cyber-sécurité des Etats-unis est très faible, voir même inexistante dans certains cas. Nous ne sommes pas les plus actifs mais certainement les plus organisés.

Qu'est ce que le piratage pour vous ?
Un défi. Si ce dernier peut aider notre pays, il se transforme en accomplissement.

Avez-vous peur des autorités ? Les lois US ne sont pas tendres !
Oui nous avons peur des autorités, mais nous avons encore plus peur quand nous nous rendons compte qu'un ennemi des Etats-unis peut attaquer nos serveurs et voler des informations sensibles de notre pays.

Avez-vous découvert des choses importantes dans vos "visites" ?
Oui, mais dévoiler les informations les plus intéressantes que nous avons découvert pourrait créer un risque pour la sécurité nationale.

Qu'est ce qui vous motive ?
Le manque de sécurité des systèmes informatiques des Etats-Unis, voilà ce qui nous motive le plus. Voilà pourquoi nous piratons de cette manière.

Quel conseil donneriez-vous à votre pays, aux autres pays, aux entreprises ?
Comprenez un pirate informatique et employez-les dans votre intérêt. Ne transformez pas tous les hackers en pirates. Nous pensons que la scène des pirates informatiques est une communauté en croissance. Sachez juste les utiliser correctement.

Et la sécurité sur Internet ?
Elle est peu sûre.

Vos premières cibles sont impressionnantes : FAA, la NASA... Vous pensez qu'elles vont réagir ?
Il y a de fortes chances, Oui.

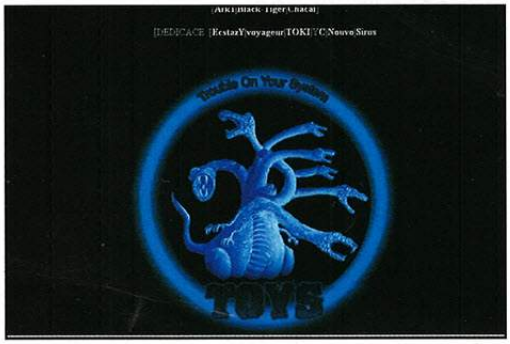
Le 11 septembre ne semble pas les avoir incité à réagir plus efficacement face aux dangers du web ?
Les attaques qui ont touché les Etats-unis ont montrées que l'informatique pouvait être plus sécurisée. Cependant il restera toujours des machines qui sont susceptibles d'être attaquées. Aux autorités d'agir. Cette situation prouve que nous sommes toujours vulnérables même après les attentats du 11 septembre. Au gouvernement de renforcer la sécurité avant qu'une attaque étrangère ne nous force à le faire vraiment.

Petits frères

Trois semaines après l'arrestation du Deceptive Duo, les administrateurs de l'Oncle Sam pensaient être tranquilles quelques mois. Raté ! Le serveur tracker.hroc.navy.mil, qui est employé pour suivre à la trace les CV et autres formulaires de demandes d'emplois a eu la visite d'un groupe nommé Infidelz. Ils ont diffusé quelques documents pour prouver leur passage. Ils ont fait le coup sur quatre autres serveurs de la Navy.

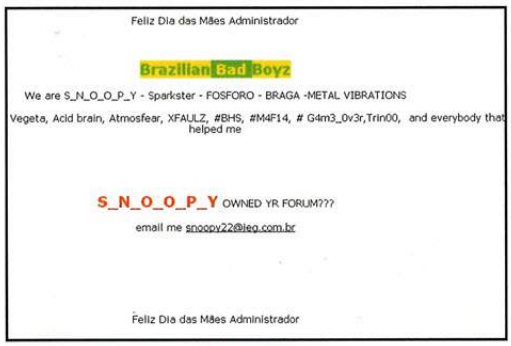
Les sites piratés du mois !

Il s'en passe de drôle sur la toile. Voici notre sélection de sites Internet piratés soit par des script-kiddies en mal de reconnaissance ou bien par des hacktivistes qui utilisent le web comme mur de propagande. Une chose est sûre, l'imagination n'est pas toujours au rendez-vous. Si jamais vous êtes témoin d'un site barbouillé, communiquez nous la capture via l'adresse contact@zataz.com

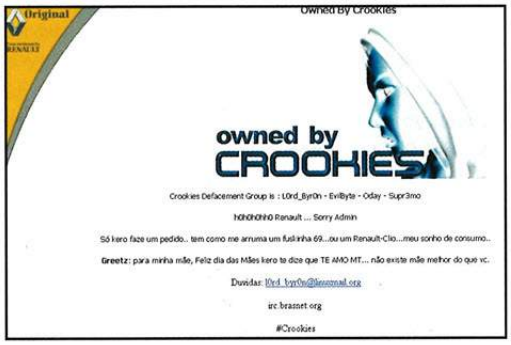


Cible : http://www.cip-sa.fr
Auteur : g0belin
Notre opinion : Rien de bien précis par ce nouveau groupe qui semble être d'origine française. Ils se sont attaqué à 7 sites sur lesquels ils ont laissé leur logo et des salutations.

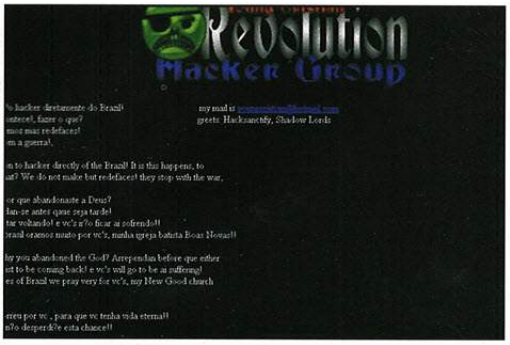
Cible : www.ferrari.co.jp
Auteur : Silver Lord
Notre opinion : Après plusieurs semaines de silence, le groupe brésilien Silver Lord est de retour en s'attaquant au site japonais du constructeur Ferrari. Les pirates n'aiment pas le rouge ? A noter qu'un un an, Silver Lord affiche prêt de 2 000 sites modifiés.



Cible : www.paysblanc.com
Auteur : Brazilian Bad Boyz
Notre opinion : Encore un groupe brésilien qui vient taquiner un site français. cette fois c'est le guide de la baule, Guérande, St Nazaire qui fait les frais du mauvais goût de ces pirates.



Cible : www.renaultoriginal.com.br
Auteur : Crookies
Notre opinion : Non vous ne rêvez pas, il va bientôt y avoir plus de pirate aux Brésil que dans tout le reste de la planète. Ce nouveau groupe de barbouilleurs s'attaque au site de Renault. Ils n'ont pas l'air d'avoir apprécié la Renault Clio là bas !

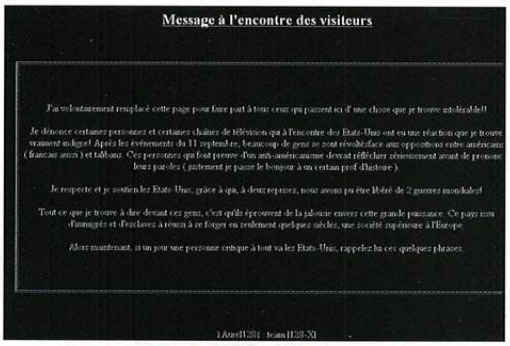


Cible : www.intelligenceonline.fr
Auteur : Young cristian
Notre opinion : Le magazine dédié à l'intelligence et aux services de renseignement a eu la visite d'un groupe de pirates brésiliens totalement inconnu appelant à la révolution...

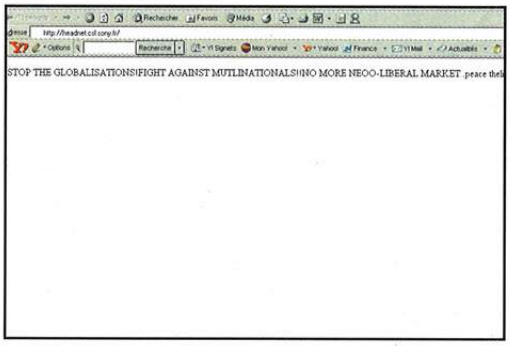
Cible : www.tracedata.fr
Auteur : Egyptian|Fighter
Notre opinion : Les hacktivistes pro palestiniens Egyptian|Fighter ont souhaité traiter de la guerre entre Israël et les Palestiniens sur le site TraceData. Photos et propos chocs au sujet des combats et des morts civils.

Cible : www.totalfianelf-ice.com
Auteur : Inconnu
Notre opinion : Ce site appartenant à Total semble avoir été la victime d'un hacktiviste qui souhaitait rappeler que l'Erika était passé par la France. En allant sur ce site, appuyez simultanément sur les touches ctrl a et vous verrez apparaître ce message : "Totalassotherapie vous offres une séance de thalasso dans la mer bretonne grâce au joie de l'ERIKA !".

Cible : www.cineinfo.fr
Auteur : Brazil hackers Sabotage
Notre opinion : Encore des brésiliens. Le Brazil Hackers Sabotage n'a qu'un seul but : Etre le premier des groupes de barbouilleurs de site internet. Nous vous proposons dans ces pages l'interview du responsable de ce groupe afin de connaître et comprendre les motivations du BHS.



Cible : www.eco2plus.fr
Auteur : }Aurel128{
Notre opinion : Un nouveau groupe français qui après un cours d'histoire semble être remonté contre ceux qui critiquent les Etats-Unis : "Je dénonce certaines personnes et certaines chaînes de télévision qui vont à l'encontre des Etats-Unis" dixit l'auteur de ce defacement.



Cible : headnet.csl.sony.fr
Auteur : Theli
Notre opinion : Theli est connu pour plusieurs piratages de taille, comme les laboratoires Pfizer. Cette fois-ci il ou elle s'attaque à un serveur de Sony France avec un message contre la mondialisation et le commerce neo libéral qui fait tant de mal.

COURRIER

Cette page est à toi cher lecteur !. Pose-nous tes questions, propose tes idées, tes remarques et nous y répondrons dans toute la mesure du possible !
Pour nous écrire, une seule adresse : contact@zataz.com

Hoax viral

J'ai reçu plusieurs e-mails me demandant d'effacer le virus Sulfnbk contenu dans ma machine. Comme vous l'indiquiez dans votre dernier numéro, je ne l'ai pas fait. Par contre je viens de recevoir un autre message avec cette fois-ce un virus nommé jdbgmgr. Que dois-je faire ?
D.D. (LYON)

Pas de panique et surtout n'effacez pas ce fichier qui existe bien dans votre système Windows. Il se trouve même dans le répertoire system32. L'effacer empêcherait votre ordinateur de fonctionner et vous seriez bon pour la réinstallation. Les auteurs de canulars manquent d'originalité ces temps ci et recyclent de vieilles idées.

M6net

"Pour vous dire que le mot de passe de M6net était diffusé sur certains chat par des pirates."
Mathieu par Courrier.
"Salut, l'accès à M6net était connu par quelques personnes car il semble qu'un ancien salarié ait diffusé le login et mot de passe sur Internet. Je n'ai pas prévenu M6Net, non pas par lâcheté, ni par envie de vouloir profiter de cet accès mais plutôt, parce que la façon dont j'avais obtenu ce mot de passe ne me donnait pas envie d'avoir à expliquer le pourquoi du comment, je n'ai nullement l'intention de me créer des ennemis ! J'ai sans doute eu tort... qui sait ?".
A.H.
"Salut l'équipe. Juste pour vous dire que votre hacker a eu son accès grâce au mot de passe diffusé sur le web"
Anonyme, Par fax.

Le moins que l'on puisse dire est que notre focus sur M6net a fait réagir quelques internautes. Des surfeurs avaient eu accès au mot de passe d'une manière différente à celle du hacker de notre article. La vingtaine de courriers que nous avons reçu nous indiquent même que ce login et mot de passe auraient été diffusés par un ancien salarié, fait que nous n'avons pas pu vérifier.

Cache-Cache

Bonjour,
Je souhaiterai cacher des documents qui se trouvent dans mon PC au travail. Que me proposez-vous ?
Plusieurs possibilités :
1/ Les copier sur une disquette, les effacer de votre pc.
2/ Les cacher en utilisant des outils de chiffrement. PGP, stéganographie, ...
3/ Utiliser un logiciel qui cachera les fichiers choisis. On vous conseille FBC : Fichiers Bien Camouflés. Téléchargeable gratuitement via www.fbc.fr.fm

Apprendre !

Salut !J'adore votre magazine et je voudrais savoir comment devenir un grand hacker.
Laurent

Nous recevons ce genre de courrier très souvent. Il faut savoir que le hacking n'a rien de magique. Ce n'est qu'une partie de l'informatique, celle qui a pour but de s'intéresser à la sécurité informatique. Je vous conseille plutôt de vous orienter vers l'apprentissage de la programmation qui vous ouvrira un jour ou l'autre une porte sur la sécurité informatique. Pour ce qui est de vous faire devenir un grand hacker, j'ai bien peur que vous finissiez petit criminel si vous n'y prenez pas garde.

Cheval de Troie

Voici quelques nouvelles informations au sujet des pirates du PMU. Parmi, des captures d'écrans de la log de sécurité de mon PC. Il y a la trace de 98 attaques illicites a partir de PC et serveurs. J'ai les nom des stations et les noms des propriétaires des stations. Il y a l'identité des personnes. Certains administrateurs ont rebondi sur des machines tiers, d'autres on utilisés des comptes de services. Je transmet ces documents à mon avocat et dispose ainsi d'éléments supplémentaires attentant qu'au PMU des individus internes au service effectuaient des manœuvres à l'encontre de ma personne et des prestataires de services. Les personnes qui ont diffusé les plans secrets du PMU, qui ont diffusés des mails et qui ont créés le site doivent être dans la liste. J'accuse le PMU d'avoir monté une machination à mon encontre et attend à ce que les magistrats en charge du dossier me demandent les pièces par le biais de mon Avocat Maître Erika KOENIG. Je dispose d'importantes charges contre le PMU et exige réparation.
Sergio Casaretto

Dans notre numéro 1, nous vous relations l'étrange affaire des pirates du PMU. Nous avons reçu par e-mail un nouveau document expliquant comme pirater le Pari Mutuel Urbain. Sergio Casaretto nous avait expliqué à cette époque comment l'informatique du PMU ne semblait pas tenir ses promesses.

Cinéma

Voila j'ai lu avec attention votre article sur la diffusion du divx et j'ai relevé quelques erreurs.

Tu es passionné(e) par l'underground, le piratage et le hacking ?
Ecris-nous pour tenter de rejoindre notre équipe !

COURRIER

SBC n'est pas une team mais une technique d'encodage du divx en 2 passes avec le codec 3.1. Vous annoncez aussi que DeCSS permet de faire tenir un DVD sur un CD de 700 mo... c'est inexact: decss permet de copier les fichiers sources du dvd (les .vob) sur le disque dur en les décryptant, pour permettre leur conversion en divx via un logiciel dédié (nandub par exemple.).

El Snyfer

Effectivement quelques petites boulettes dans notre article, ce qui ne lui enlève pas pour autant son exclusivité et son fond ! A noter que pour ce qui est du SBC, cette technique, est normalement impossible. Elle est rendue possible grâce à l'utilisation d'un logiciel nommé Nandub. Autre erreur dans notre article, par Classik, il fallait comprendre film classique.

Tu veux du boulot ?

Voila, j'ai un budget de 500 000 ff pour recruter un cracker pour juste une opération. 100.000 ff cash avant et le reste après. Si tu es un cracker très expérimenté, et que tu es intéressé, fais le moi savoir car c'est urgent. Le truc à pirater est un serveur du ministère de la justice, en fait la ou sont stockés les délits commis et effacer quelques noms précis. Ca vous intéresse ? Phateman

On va voir avec notre banquier car si on n'y arrive pas, il faut qu'on calcule le pécule qui nous sera versé à notre sortie de prison. Bien sur, on rigole, mais ce genre de courrier provenant d'un neuneu du web se rajoute à une liste qui pourrait tenir dans un hors série de 600 pages !

Virus ou pub ?

On reste un peu sur sa fin quand on lit un article comme "Bad Track". Il n'y a aucun éléments tangibles dans l'article, qui permette de s'assurer de la véracité de l'histoire de M.Royer ! Il serait intéressant de savoir au minimum quel composant est affecté afin de pouvoir déterminer plus tard si un correctif de l'éditeur vient combler la vulnérabilité (sans forcément la documenter).

On s'est posé la question. Faut-il en dire plus ou non ? Faut-il donner des éléments qui pourraient mettre sur la voix les créateurs de code viral en tout genre. Nous avons préféré la sagesse en évitant ce genre de chose. Par contre si vous êtes un professionnel, pourquoi ne pas les contacter directement ?

Pub dévorante

Bonjour, je reçois dans ma boite électronique des dizaines de messages de personnes ou d'entreprises que je ne connais pas. Que puis je faire ?

Ah les joies du spam. 40% des courriers électroniques commerciaux envoyés sur le réseau sont aujourd'hui non sollicités. Que faire ? Soit vous tentez de convaincre l'émetteur du message d'arrêter soit vous allez dans l'option message puis sélectionner "bloquer cet expéditeur" !

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)

Peur sur la F1

Est-il possible de télécommander une Formule 1 à distance ? Peut-on faire caler une voiture sur la grille de départ ? Peut-on pirater les fréquences radios entre le coureur automobile et les ingénieurs de sa team ? ZATAZ Magazine et PITSTOP Magazine, spécialiste de la F1, ont enquêtés.

Piratage ou communication ?

Les ordres qui sont transmis à la voiture lors des courses sont, en général, validés par le pilote. Les données sont donc envoyées par la voiture, analysées dans les stands, et un ordre est renvoyé à la monoplace pour effectuer tel ou tel changement de cartographie, d'optimisation moteur, de richesse d'essence, à un endroit donné du circuit. Normalement, le pilote est averti qu'une modification a été effectuée. Cette modification proposée par les ingénieurs de course se retrouve stockée dans une mémoire et seul le pilote peut valider ce changement. Le danger peut apparaître dans la mesure ou l'ordre envoyé se retrouve brouillé. Il peut y avoir une véritable confusion entre le stand et la voiture. On ne risque pas, par exemple, de voir des moteurs tourner sur 5 cylindres au lieu de 10. Où bien il y a un véritable tour de force ! Le système de communication employé est, dans son principe, semblable au GSM. Les ordres ne sont pas envoyés sur une seule fréquence mais sur plusieurs qui changent à chaque communication, ce qui restreint les risques de piratage. Ensuite, tout est contrôlé. L'ordre va vers la voiture. Une fois reçu, le stand reçoit un signal de bonne réception ainsi qu'une confirmation du pilote sur la validité de l'ordre. Au pire, le processus de modification est stoppé et le pilote roule sans... comme cela se faisait avant 1993.

Ma voiture fait crack boom huuuu !

De nouveaux règlements en Formule 1 remis à jour en 2002 permettent aux équipes d'utiliser des ordinateurs pour contrôler tous les aspects électroniques de la voiture. Cette technologie est celle de la télémétrie bi-directionnelle. *"Il y a un risque de piratage"*, a reconnu Sam Michael, ingénieur pour l'écurie Williams. *"Si le système n'est pas codé correctement, il y aura danger. De faux messages pourraient alors être envoyés. Le pire qu'il pourrait arriver serait que le moteur réagisse moins bien, mais la vie du pilote ne serait jamais en danger."* (Source : AFP). L'un des ingénieurs de chez Jordan, Gilles Flaire, un ancien fonctionnaire des services de renseignements français, croit que la télémétrie bi-directionnelle pourrait être la cible de pirates et causer *"un désastre"*. Cet ingénieur pas comme les autres était déjà apparu en 2001 quand Ron Dennis avait demandé à Bernie Ecclestone s'il savait qui espionnait l'écurie Mc Laren. Ces deux hommes auront d'ailleurs une réunion avec Gilles Flaire, qui était déjà présenté à l'époque comme un spécialiste des interceptions radio.

L'Electronique embarquée

L'électronique embarquée est blindée pour éviter des interférences électromagnétiques. Cette technologie est d'ailleurs soumise par les constructeurs à des tests CEM (Comptabilité électromagnétique). Il s'avère cependant que des problèmes peuvent apparaître. Le magazine Auto Journal, expliquait, voilà quelques temps, qu'une Mercedes Classe S s'était retrouvée clouée au parking car cette dernière avait été garée trop près d'une ligne de T.G.V. Le Forum F1Team explique quant à lui que sur l'île de Ré, le Phare des Baleines cloue lui aussi sur place les voitures sophistiquées garées à proximité. D'autres voitures, sur cette même île, voyaient la condamnation électromagnétique de leurs portes mise hors services. Pourquoi ? La puissance des ondes émises par le système Siledis de radionavigation marine perturbait l'électronique embarquée des automobiles. Ferrari, de son côté, va découvrir en 2001 que certaines perturbations touchant ses F2001 en essais a Fiorano étaient dues à l'utilisation massive de téléphones WAP par les tifosis massés à l'extérieur du circuit. Dans la même ambiance, Claudio Berro, porte-parole de la Scuderia explique : *"En rallye, il a été découvert que le pilote et le copilote coupaient le moteur lors de leurs conversations via leur radio-émetteur"*. Plutôt gênant, surtout en pleine course.

Tabou à 300 KMH

Soyons honnête, le risque est bien réel et le sujet est Tabou chez les pros de la F1 mais il faut modérer les propos de certains car les risques de piratage informatique comme nous pouvons les connaître sont relativement faibles à ce niveau de compétition. L'argent engagé, la technologie employée et un personnel ultra-compétent font qu'il y a peu de chance de voir des grand-prix sabotés par une personne tiers. Mais les systèmes codés et sécurisés sont toujours, à un moment ou un autre, faillible. Le pirate pourrait agir entre la voiture et les ingenieurs. *"La plus grande crainte des équipes n'est pas de se faire pirater et de voir les voitures "brouter" ou caler en pleine course, mais de voir les systèmes de transmission brouillés et l'interactivité entre le pilote et l'ingénieur inutilisable"* dixit un ingénieur de chez l'ex-team Prost Grand prix que nous avons interrogé pour ce reportage.

Aujourd'hui, le matériel employé par les Teams de F1 ressemble à du matériel militaire, ou d'espionnage. La parano est une partie intégrante du grand cirque de la F1 et l'on peut être certain d'entendre, dans le courant de la saison, que certaines équipes trichent ou espionnent leurs voisins... C'est monnaie courante et chaque année, le même genre d'affaire revient sur le tapis. L'année dernière une rumeur affirmait que les déboires de McLaren avaient été dus à un pirate fan d'une équipe adverse et qui, depuis le bord de piste, faisait caler les voitures sur la grille de départ. Aujourd'hui, on peut dire que c'était assez fantasque de raconter ce genre de chose tant il parait peu probable de voir ce genre d'action commise par une personne seule. Le laps de temps pour opérer est trop court et les courses durent rarement plus de deux heures. Les contrôles militaires avant la course et le fait que la procédure bi-directionnelle soit lancée au dernier moment amenuise une tentative de piratage durant la course. La probabilité de réussite d'une telle action parait très faible ou alors, via un brouillage ponctuel et personne ne s'en rendra véritablement compte. La F1 est fière comme Artaban, et un top-team n'avouera jamais s'être fait "embêtée" par un pirate, professionnel ou non. Si certains pensent regarder les Grands Prix en espérant voir des voitures "folles" rouler à contre-sens de la piste, il y a fort à parier que ce ne sera pas pour ce week-end, autant faire picoler les coureurs !

Le magazine **Net@scope** passe en grand format

Découvrez le plus populaire des magazines Internet


mag·zataz·com