NOUVEAU N°1 32 PAGES DE PIRATAGE SANS PUB

PIRAT'Z

HACKERS & GAMERS

1 Même pas dix balles !! 1,5 €

Découvrez le côté obscur d'Internet...

plantez Win à distance • warez tekniks • devenir un Hacker PRO • anonymous mail • cryptez votre HD • virus factory • triche • intrusion • ultima, everquest & co sans payer

EDITO

Pirat'Gamez est mort, vive Pirat'z ! Les lecteurs les plus observateurs auront peut-être remarqué que la première différence se situe dans la subtile disparition du "Game", et l'ajout du sous-titre révélateur "Hackers & Gamers". Eh oui : auparavant uniquement centré sur les jeux, Pirat'z s'intéresse maintenant à fond au domaine du hacking (que nous avons - après moult discussions - finalement préféré au jardinage). L'objectif est toujours, pour le côté hack comme pour le côté jeux, de rester accessible à tous, tout en vous dévoilant les secrets les mieux gardés des pirates. Vous allez enfin comprendre pourquoi votre machine plante sans arrêt (c'est votre petit frère qui s'amuse à vous nuker), pourquoi votre petit frère vous bat à Pac-Man 3D, pourquoi vous avez retrouvé dans votre chambre le CD d'un jeu qui n'est pas encore sorti (devinez qui l'a téléchargé sur Internet), ... Bref, il y en a des choses à apprendre dans ce numéro. Car si la partie hack a été rajoutée, ce n'est pas au détriment de la partie jeux ! Et oui, le contenu total a été multiplié par deux, tout simplement. Pour un prix divisé par 2,3333333... (tiens, je viens de trouver un bon truc pour remplir un édito). Où est le truc ? On est sponsorisé par Microsoft. Bon, ok, en fait on est indépendant, mais on voulait prouver qu'un mag sur le piratage original, bien rempli et pas cher, c'était possible ! Les amateurs de consoles seront peut-être un peu déçus en ne voyant pas grand chose pour leur machine préférée, mais ce n'est qu'un hasard dû aux aléas de l'actualité et de la préparation du mag. Que notre ami Sony se rassure s'il nous lit, nous continuerons à parler des modchips sur PS2... dans le prochain numéro, pour lequel je vous donne rendez-vous dans deux mois !

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
Imprimé par Imprimeries de Champagne

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

UN ÉDITEUR D'ANTI-VIRUS EXPLIQUE COMMENT FABRIQUER... DES VIRUS !

Ils étaient presque morts. Personne n'en entendait plus parler, de ces virus macro pour les logiciels Microsoft de la suite Office comme Word, Excel et Access. (Mal)heureusement, l'expert Gabor Szappanos vient de les remettre au goût du jour. Il a écrit un article qui explique comment les virus macros évolués peuvent se cacher des antivirus grâce au polymorphisme et au métamorphisme. L'auteur détaille tant ces techniques de programmation qu'on aurait presque envie d'essayer soi-même. Ce qui est amusant, c'est que l'article vient d'être publié sur le site de référence SecurityFocus.com. Or, ce site a été racheté il y a quelques mois par... Symantec, l'éditeur de Norton Antivirus ! De là à penser que cette société essaie de favoriser l'écriture de ce type de virus, pour ensuite vendre un produit qui les détectera, il n'y a qu'un pas que nous nous garderons bien de franchir.

UN ANTIVIRUS 100% EFFICACE... ET POUR CAUSE !

C'est le rêve de beaucoup d'éditeurs de logiciels anti-virus : découvrir la méthode ultime pour éliminer tous les virus connus et inconnus, sans mises à jours obligatoires. Ça existe, et c'est Symantec qui l'a trouvée. Un article de The Register paru en novembre dernier nous apprend en effet que le produit "Norton Internet Security 2003" est affecté d'un défaut de fonctionnement qui détruit automatiquement certains e-mails de l'utilisateur, même si aucun virus n'y a été détecté. Au moins, c'est efficace ! Symantec a finalement décidé de publier un correctif. Mais vous n'êtes pas obligés de l'installer...

ARRÊTÉ POUR AVOIR ÉCRIT DU CODE

En Angleterre, il ne fait pas bon être programmeur, surtout quand on s'intéresse à la sécurité informatique. Un jeune de 21 ans a été arrêté par Scotland Yard à l'issue d'une enquête qui a duré une année. Le délit dont il est accusé ? Avoir écrit des programmes et en avoir diffusé le code source sur Internet. Il est en effet l'auteur du ThOrnkit, une collection de petits utilitaires permettant à un pirate de se dissimuler sur un système Linux. Si une condamnation est prononcée, cela signifierait qu'il est illégal d'écrire un programme pouvant être utilisé à des fins illicites. Et ceci, même si l'utilisation qu'on en a fait a toujours été légale, par exemple pour tester sa propre sécurité, ou démontrer l'existence de vulnérabilités afin de permettre leur correction. Du coup, tous les spécialistes en sécurité, tous les "white hat hackers", et même les programmeurs en général, s'indignent et tremblent. En effet, quasiment tous les programmes écrits et utilisés par les sociétés de sécurité et par les administrateurs systèmes peuvent être détournés de leur usage légitime. Imaginez, même le petit programme "ping" disponible sur toutes les machines Windows pourrait être utilisé pour mener une attaque par déni de service distribué ! A quand billou en prison ?

LA DINDE SE PLANQUE AVANT NOEL

Le groupe de hackers Gobbles (qui signifie Dindon en anglais), c'est un peu le grain de sable qui enraye la mécanique bien huilée du petit monde de la sécurité. On se souvient de leurs alertes délirantes publiées sur la liste Bugtraq, soit fausses - pour prouver que les spécialistes qui modèrent les listes de diffusion sont incompétents - soit réelles et accompagnées de codes dévastateurs - quand une société de sécurité osait affirmer que la faille ne pouvait pas être exploitée par un pirate. Hélas, depuis le mois d'août, les empêcheurs de tourner en rond de Gobbles sont aux abonnés absents. Allez Gobbles, un petit effort pour Noël !

WINDOWS 98 SE MEURT, LES LIBERTÉS AUSSI

En novembre dernier, Microsoft a annoncé que l'effort de compatibilité et de sécurité sur les OS Windows 9x serait abandonné. La raison invoquée est la nécessité de se consacrer à la sécurisation de Windows XP et surtout de Longhorn, son successeur. "Les utilisateurs devront payer pour avoir de la sécurité", a expliqué Craig Mundie, le porte-parole de Microsoft. Longhorn intègrera en particu-

POURQUOI LE FIREWALL INTÉGRÉ DE WINDOWS XP NE SERT À RIEN

Grande révolution dans le monde des utilisateurs du système d'exploitation de Krosoft. Un pare-feu est maintenant intégré en standard dans Windows XP ! D'utilisation assez simple, il a été jugé efficace par les experts en sécurité. Une petite réserve cependant : il serait un peu trop basique pour un paramétrage avancé. Même s'il ne vaut pas le logiciel de filtrage intégré dans Linux depuis des années, on se sent en droit de s'extasier. Microsoft Corp. ™ ® se serait enfin décidé à sécuriser son produit phare ? Voyons... Sur les serveurs web, cela va-t-il empêcher le piratage avec les failles de IIS ? Non, car le firewall autorisera l'accès à ce service. Les virus vont-ils être éliminés ? Pas du tout, puisqu'ils se propagent par e-mail ou par téléchargements de fichiers initiés par l'utilisateur. Peut-être, alors, les attaques par chevaux de Troie seront-elles arrêtées ? Pas de chance, le firewall de Microsoft n'intègre pas cette fonction, à la différence de plusieurs de ses concurrents. Mais... Ah oui, ça va sûrement bloquer les dizaines d'attaques connues sur Internet Explorer ! Hum... devinez quoi ? Pas du tout. Conclusion, faut pas rêver, c'est pas demain la veille qu'on va pouvoir surfer couverts. Mais ne me dites pas que vous y aviez cru.

NOUVEAU CONCEPT : LE SNIFFEUR DE TROIE

Un sniffeur est un outil d'analyse réseau permettant d'espionner des communications. Tcpdump, qui fonctionne sur les plate-formes Unix, est le plus utilisé d'entre eux. Un cheval de Troie est un logiciel qui paraît inoffensif mais, en réalité, cache des fonctions dédiées à pirater ou espionner la personne exécutant le programme. Voici qu'un pirate ayant le sens de l'humour vient de réunir les deux outils ! On vient de découvrir que quelqu'un a implémenté un accès caché (backdoor) dans le code de tcpdump, disponible en téléchargement sur Internet. Ce code va donc espionner les espions… Et accessoirement les administrateurs réseau.

LE MONDE ENTIER PRIVÉ DE WEB ET D'EMAIL PENDANT 3 HEURES !

Voilà ce qui a failli arriver (eh oui, c'est pas arrivé en fait, on vous a bien eus) le 23 octobre dernier. Une attaque de déni de service d'une envergure inhabituelle a été enregistrée contre les 13 serveurs de noms principaux d'Internet. Une autre attaque identique a eu lieu fin novembre. Elle en a fait tomber la majorité pendant plusieurs heures, ce qui n'a cependant pas entraîné de conséquences visibles. Car, en théorie, il suffit d'un US envoyer des emails dans la nature sur le net pour rendre leurs rapports au commandement...

LA CERTIFICATION NE FAIT PAS LE MOINE

Le palmarès des auteurs des 510 pages de l'ouvrage "Sécurité Internet", édité par Syngress Publishing et First Interactive, est éloquent. Annoncés comme étant "exclusivement des experts en sécurité" (ce qui paraît un minimum vu le titre ambitieux du bouquin), ceux-ci totalisent à eux quatre pas moins de 21 certifications. Ces dernières sont étalées sur la couverture comme autant de gages de qualité : MCDBA, MCSE+I, CCNA, A+, Network+, I-Net+, CISSP, MCSE, MCPS, MCP+I, CNA, CMISS, CLSE, COS/2E, CLSI, COS/2I, CLSA, … Sincèrement, je n'y comprends rien, mais ça en jette. J'entr'ouvre **la bête. A** l'intérieur, première **désillusion, aucune mention de l'expérience de terrain des auteurs.** Un coup d'oeil **suffit pour voir qu'il s'agit en fait,** après un **chapitre** convenu **sur les** protocoles **réseau** et le cryptage, **d'une** sorte de manuel **dédié** aux environnements Microsoft sur **l'installation** et l'utilisation des produits commerciaux **CISCO, NAI, Check Point, ou encore AXENT…** Voilà à quoi correspondaient **ces fameuses** certifications ! **Pire, les virus et** autres **chevaux de Troie sont expédiés en deux pages,** et la **protection contre ces attaques en deux paragraphes. Ce sont pourtant là les menaces qui coûtent** le plus **cher aux entreprises. Les** auteurs auraient-ils loupé la certification MacAffe ou Norton Antivirus ?

lier Palladium, un système de protection mi-hardware mi-software qui est déjà tristement célèbre parmi les défenseurs des libertés publiques. Le niveau de sécurité additionnel, très contesté, aurait comme contrepartie le flicage des utilisateurs et l'impossibilité d'installer des logiciels non certifiés par Microsoft. On vous tiendra au courant.

SYSDOOR OU LE CHALLENGE IMPOSSIBLE

Les hackers (au sens le plus noble du terme) de l'équipe française du site sysdoor.com ont mis en ligne un serveur à pirater. Le challenge est ouvert à tous les internautes, qu'ils soient white ou black hat, professionnels de la sécurité ou simples amateurs. On peut même voir en temps réel les attaques qui sont tentées, grâce à la publication sur le site des logs du détecteur d'intrusion prélude. Sysdoor est confiant sur l'invulnérabilité du système de protection qu'ils ont inventé. D'après ce qu'on peut lire sur leur page web, la protection intègre un nouveau dispositif de cryptage annoncé comme s'inspirant du son et de l'acoustique. On n'en sait pas plus sur cette annonce alléchante. Nous, ce qu'on en pense, c'est que le site ne sera pas piraté... mais que ça ne prouvera pas pour autant qu'il est parfaitement sécurisé ! Car l'expérience montre que la "sécurité par l'obscurité" fait facilement illusion mais ne tient jamais la distance. On espère donc que sysdoor va publier ses algorithmes et ses codes sources pour pouvoir s'y attaquer sérieusement et - qui sait - valider l'idée qu'il s'agit d'une avancée majeure dans le domaine de la sécurité. En attendant, écrivez-nous, on prend les paris !

seul serveur de ce type pour faire fonctionner sur tout Internet la résolution des noms de domaine en leurs adresses Internet. Les médias se sont largement fait le relais de cette information. Mais contrairement à ce que beaucoup racontent, si l'attaque avait fonctionné à plein, le réseau Internet serait en soi resté parfaitement opérationnel. Oui, c'est vrai, le grand public ignorant aurait perdu son précieux email et n'aurait plus réussi à surfer sur le web. Mais moi j'aurais toujours pu accéder à mon serveur unix depuis un cybercafé (gnark gnark). Et toutes les communications sensibles, en particulier celles des militaires et des liaisons inter-entreprises, ne devraient pas avoir besoin de ces serveurs pour fonctionner. Pourquoi ? Le rôle des serveurs de noms est une commodité pour l'homme ; ils se bornent à faire la relation entre les noms de domaine (au texte compréhensible) et les nombres qui représentent ces adresses Internet pour les machines. Les communications sur Internet utilisent des protocoles qui n'ont besoin que de l'adresse IP du destinataire. Donc, à peu près tous les types de communications restent parfaitement possibles si on connaît cette fameuse adresse IP. Et, bien sûr, les communications sécurisées - comme c'est le cas pour les militaires et les grandes entreprises - ne se basent pas sur des noms de domaines mais sur des adresses IP fixes, avec un protocole de tunnel crypté appelé VPN. On n'imagine pas les marines

POUR UNE FOIS, LA JUSTICE AIDE LES HACKERS

Ben non, ne rêvez pas, ce n'est pas demain la veille que le piratage sera légal ! Mais dans l'immense majorité des cas, l'auteur du délit reste impuni, car aucune plainte n'est déposée. Cela a créé un manque grave de jurisprudences dans ce domaine délicat. Imaginez qu'en surfant sur le web avec votre navigateur préféré, vous tombiez (presque) par hasard sur une base de données de clients censée être confidentielle ? Pouvez-vous être accusé de piratage ? C'est ce qu'avait essayé la société Tati dans une affaire similaire, entraînant la condamnation en première instance d'un journaliste de kitetoa.com qui avait publié l'existence d'une faille élémentaire sur le site de Tati (après les avoir prévenus). Dans un rebondissement inattendu, le Parquet lui-même décidait de faire appel de la décision du juge ! En appel, Tati a été débouté de sa plainte et le journaliste relaxé. Dans l'époque paranoïaque et sécuritaire que nous vivons, cette décision, qui, on l'espère, fera jurisprudence, est une bouffée d'air frais en faveur des libertés de chacun. L'éthique hacker défendue par les tribunaux ? Aaahh... ça fait du bien :-)

UN UTOPISTE CHEZ MICROSOFT

Michael Howard est un employé de Microsoft. Il intervient dans un ambitieux projet intitulé "Secure Windows Initiative". L'homme semble de bon niveau et décidé à agir concrètement. Mieux, il publie certains de ses résultats sur Internet, n'hésitant pas à donner des exemples de trous de sécurité qu'il a corrigés sur Windows, et même des bouts de code source ! Sur la célèbre liste de diffusion bugtraq, il est à l'origine d'une discussion constructive permettant de limiter l'impact des failles de cross-site scripting en empêchant le vol des cookies. Après des années de boycott et d'attaques verbales, cette initiative individuelle indique-t-elle que Microsoft va passer dans le camp de l'open-source et du "full-disclosure" ? Dans Pirat'Z numéro 60, nous referons un point sur le sujet.

ÉCHANGE 0-DAY CONTRE 900 DOLLARS

Vous avez découvert un 0-day, c'est-à-dire un trou de sécurité encore inconnu du public ? Ou alors, vous avez écrit un code permettant d'exploiter une vulnérabilité connue ? Dans les deux cas, cher ami hacker, vous pouvez gagner entre 300 et 900 euros en vendant votre âme sur www.idefense.com/contributor.html. Une fois en possession de votre travail, cette société de sécurité informatique va le revendre à ses clients privilégiés. Après un certain temps, elle diffusera l'information au public. Un sondage du site packetstorm.linuxsecurity.com indique que 30% des votants pensent que cette initiative va stimuler la diffusion des 0-days (et donc améliorer la sécurité). Nous, on est plutôt du côté des 18% qui considèrent que ça risque de tuer l'information gratuite.

DO IT !

PIRATER UN SERVEUR EN DEUX CLICS

Tous les jours, des dizaines de sites web voient leur page d'accueil modifiée par des pirates. Souvent, ces défaçages sont réalisés par des groupes de jeunes script-kiddies sans grande compétence technique. Ils trouvent et exploitent des trous de sécurité en utilisant des outils automatisés qui font tout le travail à leur place !

APACHE UNDER ATTACK

Le serveur web gratuit Apache, qui se cache derrière plus de la moitié des sites web du monde, a toujours eu une excellente réputation de sécurité. Il se riait des failles unicode et autres dépassements de tampons de son concurrent direct, le serveur IIS de Microsoft. Pourtant, ces derniers mois, l'indien a perdu quelques plumes. Au milieu de l'année 2002, le groupe Gobbles avait déjà entamé l'offensive en publiant un exploit fonctionnel qui a obligé nombre d'administrateurs à corriger dans l'urgence. Par la suite, plusieurs chercheurs ont révélé la possibilité d'attaques sur les modules, les bibliothèques de fonctions, et les logiciels annexes. Il est vrai que le code source d'apache est excellent et très bien audité. Mais, afin de fournir certaines fonctionnalités, le serveur fait appel à des fonctions ou programmes externes, souvent écrits par d'autres personnes... Ce qui compromet la sécurité. Citons l'existence de dépassements de tampon sur le module PHP gérant les uploads de fichiers et sur les routines de chiffrement SSL, une vulnérabilité de type cross-site scripting, et de nombreuses failles exploitables localement ou en environnement de type serveur mutualisé.

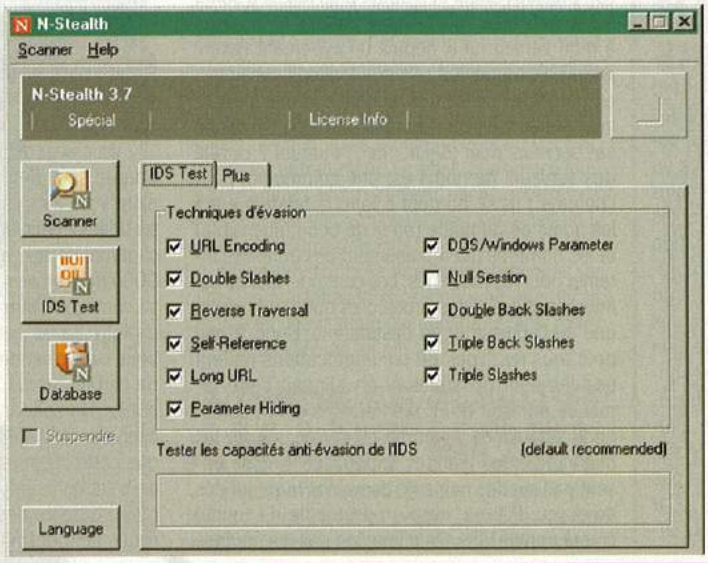
SCANDALE : PAS D'ISOLOIR POUR LE VOTE EN LIGNE À L'UMP !

C'est en tout cas dans ces termes que Nicolas Dupont-Aignan, député de l'Essonne et candidat malheureux avec 15% des voix, a qualifié le vote en ligne destiné à élire le représentant du principal parti de droite. Il dénonce l'absence d'isoloirs et " l'organisation très aléatoire " du vote des militants qui avaient reçu par la Poste leur identifiant et leur mot de passe pour voter en ligne. Avec seulement 30% de participation, il est sûr en tout cas que cette expérience inédite de vote par Internet est tout sauf réussie...Ridicule

C'est une triste réalité, mais il vaut mieux bien la connaître. On pourrait croire que ces logiciels sont très difficiles à trouver et ne circulent que dans les milieux les plus fermés de l'underground. En réalité, s'il est vrai que les programmes de "mass-rooting" et les "auto-rooters" sont rarement publics, les meilleurs utilitaires de détection de vulnérabilités sont disponibles en téléchargement pour tous sur le web.

Paradoxe ? La plupart des logiciels de détection automatique de trous de sécurité sont créés et diffusés par des entreprises américaines de sécurité informatique. Elles fournissent aux internautes des versions d'évaluation complètes. En fait, ça sert aux administrateurs systèmes qui souhaitent vérifier la sécurité de leur réseau. Mais ces programmes font aussi la joie des pirates en herbe, car ils fonctionnent sous Windows, avec une interface intuitive. Il suffit d'inscrire dans la case dédiée le nom ou l'adresse IP du (ou des) serveur(s) à attaquer, et de cliquer sur le bouton "démarrer le scan". Le logiciel vérifie alors sur le serveur l'existence ou non des dizaines de milliers de vulnérabilités connues. Quelques minutes plus tard, le pirate possède un rapport complet sur les failles potentielles de sa cible, avec le degré de gravité. En fonction du résultat, il décide de changer de cible ou d'attaquer.

Si le pirate choisit l'attaque, il va rechercher un petit programme (appelé "exploit") qui permettra d'utiliser une des failles détectées pour rentrer dans le serveur. Les script-kiddies n'ont souvent pas les compétences pour écrire leur propres exploits, ils vont les chercher sur un site spécialisé, comme PacketStorm (packetstormsecurity.nl). L'autre possibilité est de tout automatiser, et pour cela d'utiliser un logiciel qui essaie d'exploiter automatiquement les failles qu'il détecte. Comme nous l'avons vu, ces utilitaires sont plutôt réservés à l'underground, mais il existe quelques tentatives publiques, comme Remote Access pour Linux (salix.org/raccess/) et Fluxay pour Windows (www.netxeyes.org/down.html).



LES MEILLEURS OUTILS DE DÉTECTION DE FAILLES

Nessus (www.nessus.org) est un excellent logiciel d'audit de vulnérabilités sur tous types de serveurs et d'équipements réseaux. Il fonctionne sous Linux et autres Unix. Il possède une interface graphique, il est gratuit, libre (license GPL opensource), et réalisé par un français : Renaud Deraison. On a également la possibilité d'écrire ses propres plugins. C'est LE must, mais réservé aux initiés.

NStealth fonctionne sous Windows avec une interface graphique facile à utiliser. Ce logiciel est commercial, mais une version gratuite pleinement fonctionnelle est téléchargeable sur le

site de la société Nstalker (www.nstalker.com/dwform.php). Il est spécifiquement orienté vers la (non) sécurité des serveurs Web, en mettant l'accent sur les vulnérabilités des scripts CGI, les failles ASP, PHP ou encore Unicode parmi les 19000 failles testées. Il propose même d'utiliser des techniques de furtivité pour échapper aux détecteurs d'intrusion !

Shadow Security Scanner est l'outil le plus complet, et aussi le plus dangereux. Il combine l'universalité et la polyvalence de Nessus avec la facilité d'utilisation de Nstealth, en rajoutant quelques fonctionnalités fort intéressantes. Ainsi, on peut réaliser le scan de manière anonyme en utilisant un relais (proxy Socks ou HTTP). Le logiciel permet aussi de spécifier des fichiers de mots de passe pour essayer de cracker en direct les comptes administrateurs des FTP ou des machines Windows (grâce aux partages cachés NetBIOS, merci Billou !). Bref, un outil à ne pas mettre entre toutes les mains... mais dont une version gratuite est disponible officiellement sur le Net sur le site de la société éditrice www.safety-lab.com. Vous êtes prévenus!

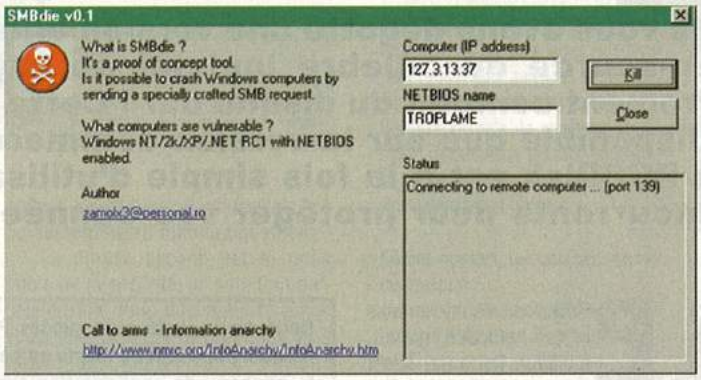
CUM Security Toolkit, alias CST, est un outil en ligne de commande développé sous Java pour le groupe de hackers du site blackhat.be. Il fonctionne aussi bien sous Windows que sous Linux. Ce scanner de failles de scripts CGI a la particularité de proposer 11 méthodes différentes pour contourner les détecteurs d'intrusion et camoufler l'attaque dans les logs du serveur...

À vous de jouer maintenant, en essayant ces programmes sur vos serveurs avant qu'un pirate ne le fasse. Attention, on vous rappelle que le simple scan de ports d'un ordinateur ne vous appartenant pas est considéré comme illégal, même si vous n'avez aucune intention de réaliser une attaque. Il existe d'autres outils très performants, en particulier pour l'intrusion dans les serveurs Web, mais nous allons nous arrêter là pour cette fois. Rendez-vous au prochain numéro !

Script kiddies DO IT!

PLANTER WINDOWS XP A DISTANCE

Vous vous souvenez tous du NUKE, une technique qui permettait de planter n'importe quelle machine sous Windows 95 en faisant apparaître un joli écran bleu. On croyait ce fléau définitivement relégué au rang des antiquités, mais il revient en force



Le nuke, ça rappelle le bon vieux temps. Quand les patches de sécurité de Windows n'existaient pas, quand on était encore innocents et naifs, qu'on chatait tranquillement sur irc et que soudain on voyait son ordinateur ralentir, la souris se figer, le disque dur mouliner follement avant de s'arrêter, vaincu. À l'origine de ce problème, un trou de sécurité sur le système de partage des fichiers sur le réseau utilisé par Windows. Il suffisait d'envoyer un paquet particulier par Internet sur l'adresse IP de la victime, à destination du port 139 (le port du partage windows, qui est activé par défaut), et la machine distante plantait misérablement.

On croyait ces temps révolus, les correctifs de Microsoft ayant éliminé le bug permettant de nuker nos pires ennemis. Avec Windows XP, le plus sécurisé de tous les Windows d'après Microsoft, on ne s'attendait pas à voir ressurgir un tel problème. Et pourtant... un chercheur en sécurité informatique a révélé l'existence d'un bug sur le partage de fichiers de Windows, qui permet de tuer la machine distante par l'envoi d'un seul paquet sur le port 139 ! Le problème existe sur toutes les machines possédant le système d'exploitation Windows NT, 2000 et XP, ayant le partage de fichiers activé. Oh oh... Il n'en fallait pas plus pour qu'un script-kiddie se faisant appeler zamolx remette le nuke au goût du jour. Il a écrit un petit programme qui permet à n'importe qui d'éliminer les personnes qu'il n'aime pas. Il suffit pour cela d'entrer l'adresse IP de la victime dans la case dédiée, et son nom de partage Netbios, puis de cliquer sur le bouton "kill". Cela ne nécessite pratiquement aucune connaissance technique, car même les pires lamers savent obtenir une adresse IP. Et à partir de là le nom Netbios s'obtient immédiatement, par exemple avec la commande du DOS "nbtstat -A adresse_ip".

Heureusement, Microsoft a fourni des correctifs permettant de se protéger de ce bug. Si vous avez installé les dernières mises à jour avec Windows Update, vous n'êtes pas vulnérables. A priori. Par mesure de prudence, nous vous conseillons de le vérifier en téléchargeant ce petit outil sur le net et en l'essayant sur votre propre ordinateur. Attention, pensez auparavant à fermer toutes les applications en cours et à sauvegarder vos données.

J'ai quand même une question à 100 000 euros à vous poser : "que va-t-il se passer quand les gens n'oseront plus mettre leur système à jour de peur de voir débarquer les policiers chez eux ?" En effet, la politique anti-piratage de Microsoft commence à se durcir. Pour les dernières versions de Windows XP, la mise à disposition des correctifs par Internet est d'ores et déjà réservée aux individus ayant réellement acheté le produit. Les déteneurs d'une copie pirate, si nombreux en France, ne pourront plus se sécuriser. Cela va-t-il entraîner un rebond des ventes de ce système d'exploitation, un passage à Linux, ou une augmentation dramatique du nombre de machines non sécurisées connectées en permanence à Internet par l'ADSL ?

1Z

ARRIVÉE DES VIRUS SUR VOS CELLULAIRES

Aux USA, certains mobiles intègrent déjà une machine virtuelle Java. Cela signifie qu'ils sont capables d'exécuter du code que l'utilisateur aura téléchargé. C'est donc la porte ouverte à toutes les calamités existant sur PC, comme les virus, les chevaux de Troie, et les logiciels espions. C'est vrai, en France, on ne les verra sans doute pas avant un an ou deux. Mais ne soyez pas déçus : vous pouvez déjà acheter à la FNAC de ravissants petits téléphones-organiseurs qui tournent sous Windows CE. Voilà qui va faciliter la tâche des créateurs de virus !

LE DMCA RETOUCHÉ ?

Aux Etats-Unis, le Digital Millennium Copyright Act a fait couler beaucoup d'encre. Pas qu'aux Etats-Unis d'ailleurs, dans Pirat'z aussi ;) En tout cas, le Bureau Américain du Copyright est actuellement en train d'accepter des commentaires critiques sur une des sections les plus controversées : celle concernant l'interdiction de contourner une protection. Bon, pour l'instant, ils ne font qu'écouter, il n'y a pas de date prévue pour la modification de la loi. Mais c'est déjà un début. On espère que les pays Européens s'apprêtant à intégrer l'EUCD dans leur législation prêteront une oreille attentive à ces remarques.

EXCLUSIF

Hum, au fait, on a quelque chose ? Khan ? Ah. Bon. Heu... Non, en fait, il va falloir que vous reveniez dans deux ou trois mois. On n'a rien de totalement exclusif pour le moment. Désolé. Remarquez, nous au moins on ne fait pas semblant ! (notez ici l'attaque subtile contre certains de nos confrères) (remarquez également l'usage démagogique et cynique du terme "confrère", qui est une parabole hypocrite communément utilisée à la place du mot "concurrent") Je sais on s'en fout, mais il y avait un trou dans la maquette ;)

Protection ultime

CRYPTEZ VOTRE PGPDISK

DO IT ! Nous vous avons dégotté une version entièrement gratuite et open-source du célèbre logiciel de cryptage PGP, et qui intègre le chiffrement complet du disque dur ! Cette fonctionnalité n'est normalement disponible que sur la version commerciale payante. Nous allons voir que PGPDisk est à la fois simple d'utilisation et plus efficace que ses concurrents pour protéger vos données des regards malveillants.

IZ

MICROSOFT DÉBORDÉ PAR SES FAILLES

Eh oui : vous pouvez attraper un virus, ou même vous faire pirater à distance, rien qu'en surfant sur le Web... et ceci même si vous avez installé les derniers correctifs de sécurité de Microsoft ! Une ribambelle de trous de sécurité à été découverte sur "IE". Débordée, l'équipe de Microsoft n'arrive pas à tout corriger. À force de se contenter de parer au plus pressé, elle finit par laisser des trous énormes. Des white hat hackers, comme http-equiv du site malware.com, l'ont prouvé en mettant en ligne des pages web de démo. Visionnées, elles-ci installent un programme sur votre disque dur et l'exécutent automatiquement ! Il est temps de passer à Opera.

BIG FAILLES SUR LES TRANSPORTS AÉRIENS US

Les tests de sécurité informatique menés par les enquêteurs du Congrès n'ont été guère probants. Depuis trois ans, les agences gouvernementales sont toujours aussi perméables aux cyber-attaques, alors que celles-ci ont gravement augmenté ces dernières années (97 000 en 2002 contre 4000 en 1998). Arrive en tête des mauvais élèves le Département du Transport avec une note de 28 sur 100. Ce qui est assez inquiétant, vu que ses systèmes informatiques règlent les vols commerciaux...

PGPDisk se résume en trois mots : efficace, gratuit, meilleur. Pourtant, il est trop peu connu. Nous allons dans cet article combler cette lacune, et vous faire découvrir un logiciel puissant et simple à utiliser, qui bénéficie de l'expérience des développeurs du célèbre programme de cryptage PGP.

Nous avons testé avec succès PGPDisk sous Windows 98 et 2000. Mentionnons tout de même un petit bug sur notre 98, qui rajoute dans le panneau de configuration système un grand nombre de volumes PGPDisk fantômes. Sous Windows XP, le logiciel PGPDisk devrait également fonctionner, mais nous ne pouvons le confirmer pour ce qui est de la version gratuite (on l'avoue, on n'a pas Windaube XP à la rédac !). Après tout, si vous en faites une grosse utilisation, payer pour obtenir la dernière version de cet excellent programme est très certainement une idée gagnante.

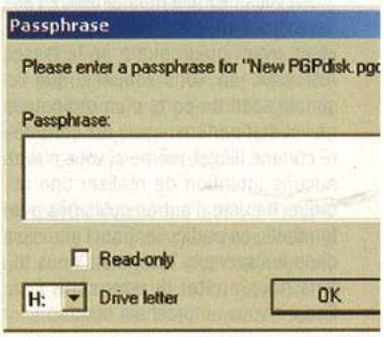
Sur votre disque dur, vous stockez des fichiers, des documents, des images. C'est confidentiel ou tout simplement personnel. Vous ne souhaitez pas, et c'est votre droit le plus intime, qu'ils soient consultables par tout le monde : votre patron, votre secrétaire, votre famille, un éventuel pirate ou un voleur d'ordinateur portable... Quelles mesures prendre pour en assurer la confidentialité ?

La première idée qui vient à l'esprit est de mettre un mot de passe sur vos documents. Mais là, attention danger ! Par exemple, les mots de passe des documents de la suite Office de Microsoft sont cassables très facilement, car les algorithmes de cryptage utilisés sont beaucoup trop faibles. Il existe sur Internet des petits programmes qui cassent ces prétendues protections quasi instantanément. Quand aux autres "solutions" de sécurité proposées par la firme de Redmond, comme le système de fichiers encrypté EFS, on se souvient du passé assez désastreux de Microsoft sur le plan de la sécurité : on ne l'utilisera donc que lorsque l'implémentation ne sera plus propriétaire. Le premier avantage des logiciels de la suite PGP, c'est en effet que leur code source est disponible (au moins pour les versions que nous allons utiliser). Ce qui permet aux experts du monde entier de vérifier que les algorithmes de chiffrement sont bien implémentés, et qu'il n'y a pas de vulnérabilités dues à des bugs dans le code.

UN FICHIER EN CLAIR NE PEUT JAMAIS ETRE COMPLÈTEMENT SUPPRIMÉ

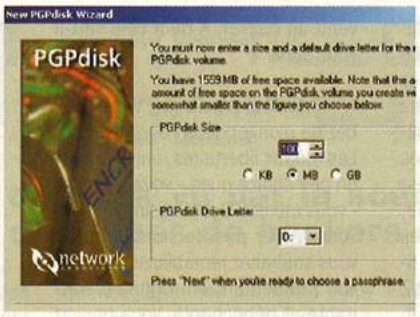
Bon, le cryptage au coup par coup des fichiers, ça fonctionne, mais ça n'est pas très pratique. La meilleure solution, à la fois plus simple d'utilisation et plus sécurisée, c'est carrément de crypter toute une zone de votre disque dur ! C'est ce que va faire pour vous le logiciel PGPDisk. Il est inclus dans la version commerciale du logiciel PGP de cryptage d'e-mails, mais également (et c'est un scoop qu'on vous offre ici) dans la version 6.0.2i de PGP freeware, qui est téléchargeable gratuitement sur le site international www.pgpi.org. Allez directement sur l'adresse : http://www.pgpi.org/cgi/download.cgi?filename=PGPfreeware602i.exe. Attention, seule cette version particulière de PGP freeware possède PGPDisk. Au niveau de la légalité, le chiffrement est à clé symétrique de 128 bits (l'équivalent du plus haut niveau de cryptage sur les sites web d'Internet), donc il devrait être autorisé en France. Néanmoins nous ne vous donnons pas de garantie sur ce point.

Certains programmes du commerce, chers payés, vont vous chiffrer tous les fichiers contenus dans des répertoires spécifiés de votre disque dur. Au démarrage de l'ordinateur, le logiciel va prendre quelques secondes (ou quelques minutes, c'est selon) pour tous les déchiffrer, vous permettant ainsi d'y accéder. À l'extinction de votre machine, les fichiers sont de nouveau chiffrés et les fichiers stockés "en clair" sont supprimées du disque. Cette procédure n'est pas bonne ! Le simple fait de stocker les fichiers en clair sur le disque dur à chaque reboot peut être un grave



DISQUE DUR AVEC

manquement à la sécurité. En effet, un fichier en clair ne peut jamais être complètement supprimé une fois qu'il a été écrit sur le disque, des logiciels (ou des machines plus ou moins sophistiquées) peuvent le récupérer en tout ou en partie. Un des gros avantage de PGPDisk est qu'il limite au maximum l'exposition de vos données sensibles en ne les déchiffrant que sur demande, lorsque vous cliquez sur le nom d'un fichier pour y accéder. Tous les autres fichiers restent cryptés. Cette méthode a aussi comme avantage l'absence de temps d'attente au démarrage.



CRYPTONS, CRYPTONS !

Comment ça marche ? C'est très simple. Après avoir suivi la procédure d'installation standard de PGP Freeware 6.0.2i, vous vous retrouvez avec une version de PGP installée sur votre machine. Dans le menu Démarrer, Programmes, PGP, vous pouvez exécuter l'utilitaire PGPDisk. Celui-ci vous servira à gérer vos partitions virtuelles encryptées, appelées "volumes PGPDisk". Un volume PGPDisk est en fait un gros fichier unique, que vous pouvez placer n'importe où sur le disque en lui donnant l'extension que vous désirez. Cliquer sur "New" permet de créer un nouveau volume. Vous devrez en spécifier la taille, qui sera la taille maximale totale des fichiers encryptés contenus dans le volume. Vous devrez également choisir un mot de passe, ou plutôt une phrase secrète, qui servira à chiffrer et déchiffrer le volume.

Après avoir recueilli des données aléatoires pour générer la clé de cryptage, grâce aux mouvements de votre souris, le programme vous demandera de formater le volume nouvellement créé et de le nommer. Vous êtes maintenant l'heureux possesseur d'une partition cryptée vierge, sur laquelle vous allez pouvoir copier vos fichiers confidentiels, ce qui les protègera automatiquement.

La phrase secrète est le point faible de la sécurité, un soin tout particulier doit donc être apporté à son choix. Elle doit être à la fois facile à retenir et impossible à deviner. Prenez une phrase suffisamment longue et originale, que vous n'utilisez pas déjà ailleurs, en rajoutant quelques chiffres et divers symboles. Gardez à l'esprit qu'il existe des programmes de crack utilisant des dictionnaires de citations !

Lorsque vous activez un volume crypté en cliquant sur "Mount", PGPDisk vous demande votre phrase secrète. Ensuite, il installe un gestionnaire de disque qui fait croire au système qu'un nouveau disque dur existe. Il apparaîtra par exemple avec la lettre "H:" dans l'explorateur windows. En réalité, tous les fichiers que vous allez copier ou lire sur H: sont inclus de manière chiffrée dans l'unique gros fichier que vous avez créé au début. C'est le gestionnaire installé par PGPDisk qui fait l'intermédiaire et donne l'illusion au système d'une nouvelle partition non cryptée. Quand vous en avez fini avec vos données privées, n'oubliez pas de cliquer sur "Unmount" pour enlever l'interface H : d'accès non crypté. Personne ne pourra plus alors accéder à vos fichiers protégés s'il ne possède pas votre phrase secrète !

Ce logiciel possède bien d'autres fonctionnalités que nous vous laissons découvrir par vous-même. Notons en particulier la possibilité d'ajout d'autres phrases secrètes pour ouvrir le même volume, bien pratique en cas d'oubli (on peut stocker la phrase secondaire dans un lieu sûr), et les divers raccourcis et automatisations pour les fonctions "Mount" et "Unmount".

"LES PLUS SÉCURITÉ DE PGPDISK"

Le manuel de PGP est édité par la société NAI et traduit de manière non officielle par les volontaires courageux du groupe de discussion fr.misc.cryptology. Ils nous expliquent les mesures mises en oeuvre par PGPDisk pour améliorer la sécurité. Par rapport aux logiciels concurrents, PGPDisk possède de nombreux avantages, illustrés dans plusieurs passages de ce document de référence que nous avons compilés et résumés ici :

MEME OUVERT, UN VOLUME PROTÈGE ENCORE :
sauf si un fichier ou une application sont en cours d'utilisation, ils y restent cryptés. Si votre ordinateur devait planter pendant qu'un volume est ouvert, son contenu restera crypté. Bien que les volumes que vous créez avec PGPdisk fonctionnent exactement de la même façon que les disques avec lesquels vous avez l'habitude de travailler, les données sont en réalité conservées dans un grand fichier crypté. Toutes vos données demeurent sécurisées dans le fichier crypté et ne sont décryptées que lorsque vous accédez à l'un de ces fichiers.

PHRASES SECRÈTES.
Les produits PGP vous encouragent à utiliser une phrase entière ou une longue série de caractères pour protéger vos données sensibles. De telles phrases secrètes sont en général plus sûres que les traditionnels mots de passe de 6-10 caractères.

CHIFFREMENT.
Il a recours à une formule mathématique sûre pour brouiller vos données de sorte que personne d'autre ne puisse les utiliser. Quand vous appliquez la bonne clé mathématique, vos données redeviennent intelligibles. Le processus de chiffrement de PGPdisk est une formule mathématique complexe appelée CAST. Il existe de solides arguments permettant de penser qu'il est complètement immunisé aussi bien contre la cryptanalyse linéaire que différentielle.

[PGPDISK PERMET DE] SÉCURISER LE CONTENU DE SUPPORTS EXTERNES,
tels que des disquettes ou des cartouches de sauvegarde. La possibilité de crypter un support externe ajoute à la sécurité pour la conservation et l'échange d'informations sensibles. Quand l'option AutoUnmount est cochée, PGPdisk ferme automatiquement tous les volumes PGPdisk ouverts si votre ordinateur est inactif pendant le nombre de minutes indiqué. Vous pouvez saisir une valeur de 1 à 999 minutes.

EFFACEMENT DE LA PHRASE SECRÈTE.
Quand vous saisissez une phrase secrète, PGPdisk ne l'utilise que pour un temps très bref, puis l'efface de la mémoire. Ce dispositif est essentiel – si la phrase secrète restait en mémoire, quelqu'un pourrait l'y récupérer si vous vous éloigniez de votre ordinateur. A votre insu, on pourrait alors accéder à n'importe quel volume PGPdisk protégé par cette phrase secrète.

PROTECTION RELATIVE À LA MÉMOIRE VIRTUELLE.
Votre phrase secrète ou d'autres clés pourraient être écrites sur le disque dur par le biais du fichier d'échange de la mémoire virtuelle. PGPdisk veille à ce que les phrases secrètes et les clés ne soient jamais écrites sur le disque. Ce dispositif est important parce que quelqu'un pourrait examiner le fichier de mémoire virtuelle à la recherche de phrases secrètes.

PROTECTION CONTRE LA RÉMANENCE ÉLECTROSTATIQUE EN MÉMOIRE VIVE.
Quand vous ouvrez un PGPdisk, votre phrase secrète est transformée en clé. Cette clé est utilisée pour crypter et décrypter les données dans votre volume PGPdisk. Tandis que la phrase secrète est immédiatement effacée de la mémoire, la clé (de laquelle votre phrase secrète ne peut pas être dérivée) y demeure pendant que le disque est ouvert. Cette clé est certes protégée de la mémoire virtuelle; cependant, si une certaine zone de la mémoire [vive] stocke exactement les mêmes données pendant de très longues périodes sans être éteinte ou réinitialisée, cette mémoire tend à conserver une charge statique, qui pourrait être lue par des attaquants. Si votre PGPdisk reste ouvert pendant de longues périodes, avec le temps, des traces discernables de votre clé pourraient demeurer en mémoire. Les grands Etats sont susceptibles de posséder des outils permettant de réaliser cette attaque. PGPdisk se protège de ça en conservant deux copies de la clé en RAM, une copie normale et une copie bit inversé, et en intervertissant fréquemment les copies.

COMMENT DEVE

Comment faire pour devenir un hacker ? Voilà sans aucun doute la question qui est la plus posée sur les forums de discussion à connotation underground d'Internet. Généralement, aucune réponse constructive n'est apportée à cette question trop classique et trop imprécise. Pourtant, même si l'objectif est aussi difficile à atteindre qu'il y paraît, il reste dans le domaine du possible. Notre dossier n'a évidemment pas la prétention de faire de vous un hacker, mais il vous donnera les pistes indispensables pour comprendre les possibilités qui s'offrent à vous et éviter les embûches.

QU'EST-CE QU'UN HACKER ?

Le sens de ce mot est très controversé. Pour les puristes, un hacker est un passionné spécialiste des ordinateurs, des réseaux, de la programmation... C'est effectivement le sens initial du mot. De son côté, le sens populaire imposé par les médias affirme qu'un hacker est un pirate informatique. Le premier article de notre dossier va éclaircir les significations multiples de ce terme, et faire la distinction entre différents types de hackers.

Quand nous parlerons de "hacker" dans le reste du magazine, ça sera pour désigner une personne très compétente en informatique et en programmation, qui est également passionnée de sécurité informatique et aime à chercher comment on peut la contourner. Les pirates informatiques compétents rentrent tous dans cette catégorie, mais ils sont rares, la majorité des pirates étant des script-kiddies au savoir quasiment nul.

Vous aurez donc compris la première leçon, qui est la plus importante : tout individu possédant un minimum de neurones, quel que soit son âge, peut devenir un bon hacker... à condition qu'il prenne le temps d'apprendre. Lire des docs, programmer, installer des systèmes d'exploitation les plus divers, créer un réseau local chez soi, faire des tests, lire Pirat'Z, et recommencer. Comptez au minimum un an, voire deux, pour arriver à un niveau correct. Rassurez-vous, le processus d'apprentissage est ce qu'il y a de plus passionnant dans la vie d'un hacker, d'ailleurs il ne s'arrête vraiment jamais et c'est tant mieux. Le risque est que vous vous preniez pour un caid au bout de quelques mois parce que vous arrivez à utiliser quelques outils et à défacer des serveurs web de Microsoft. C'est comme cela que les script-kiddie, cette plaie des temps électroniques modernes, se créent. Rien qu'en lisant ce premier numéro de Pirat'Z je suis sûr que vous atteindrez un niveau honorable de script-kiddie : mais votre but est d'aller plus loin, n'est-ce-pas ? D'apprendre, et de comprendre en profondeur les choses... Ce qui nous mène à :

LA PHILOSOPHIE DU HACK

Tout le monde a entendu parler de la philosophie des premiers hackers, des puristes, initiée par des gens comme Richard Stallman. Parmi leurs idées, on trouve la libre diffusion de l'information, le logiciel libre (vous savez, la Free Software Fundation et sa license GPL), et le droit inaliénable du hacker à passer ses nuits devant un écran comme l'associal qu'il est.

Mais c'est d'une philosophie plus radicale dont nous allons vous parler dans le second article de notre dossier. Les idéaux du monde de l'underground, incarnés dans le célèbre "Manifeste du Mentor". Ceux qui estiment que, sur les réseaux, l'information est si fondamentalement libre qu'il est du droit de chacun d'y accéder, et que s'introduire dans un serveur protégé pour en extirper une donnée cachée est un acte légitime.

Croire en une certaine philosophie du hack n'est pas nécessaire pour devenir un bon hacker. La passion, sans raison éthique profonde, se suffit à elle-même. Souvent, les apprentis pirates se justifient de leurs intrusions en invoquant une philosophie de la liberté universelle de l'information à laquelle il ne comprennent rien. Une prétendue "soif d'apprentissage", qui pourrait pourtant s'étancher par d'autres moyens, est le prétexte qui tente de justifer toutes leurs actions.

QUELS DÉBOUCHÉS POUR LES HACKERS ?

Félicitations, vous avez beaucoup lu et beaucoup appris, avec humilité et passion, vous êtes devenu un hacker. À quoi cela va-t-il vous servir ?

Première possibilité, vous décidez de plonger dans l'underground. Les idéaux libertaires, universels et un peu anarchiques - voire nihilistes - vous attirent. Ou, plus simplement, vous n'avez pas de sens moral et vous souhaitez rentabiliser votre savoir rapidement en monnaie sonnante et trébuchante. Vous pouvez alors prendre un petit boulot le jour et vivre la nuit devant votre écran. Mais attention de ne pas vous laisser entraîner trop loin. Notre article sur les lois en vigueur en France (qui devraient être renforcées prochainement) vous donnera un aperçu de ce qui vous attend inévitablement.

Il existe une seconde possibilité, bien plus intéressante, qui permet de gagner sa croûte en vivant sa passion légalement : devenir un hacker professionnel. Oui, ça existe ! Notre article vous exposera les différents débouchés possibles. Il conclura sur l'interview édifiante de Thor, un hacker américain qui réussi.

TECHNIQUES D'ATTAQUE

A l'issue de la lecture de notre dossier, vous aurez certainement une bonne idée de ce qu'est un hacker et des moyens d'en devenir un. Ce que l'on ne peut pas vous donner d'un seul coup, c'est l'expérience et les connaissances. Il vous faudra apprendre par vous-même ! Mais nous allons vous y aider, dans une modeste mesure, dans la suite de ce magazine (et aussi, bien sûr, dans les numéros suivants). Vous y découvrirez en particulier certaines techniques offensives utilisées par les pirates. C'est là que vous pourrez tester votre véritable volonté d'être un hacker et pas un bête script-kiddie, en testant ces techniques sur votre propre ordinateur, en essayant de comprendre leur fonctionnement, en analysant les programmes... Évidemment, nous vous déconseillons d'essayer d'attaquer des serveurs sur Internet : nous n'expliquons pas dans ce numéro les techniques permettant de passer inaperçu ; votre attaque aura de grande chance d'être détectée et vous d'aller devant un tribunal. Ça serait dommage...

LA CYBER-VENGEANCE SE MANGE FROID

Une jeune femme iranienne, étudiante à Téhéran, a payé cher son refus d'épouser l'homme qui la convoitait : dépité, le prétendant, vendeur de matériel informatique, a eu la bonne idée de mettre des photos sur le Web de la demoiselle... complètement nue ! L'amoureux éconduit avait en réalité utilisé des photos du visage de l'étudiante de 21 ans, prises lors d'une fête d'anniversaire, qu'il avait mises sur les corps dénudés d'autres femmes. Il avait quelques jours plus tard appelé la donzelle pour lui donner l'adresse d'un site à consulter. Se voyant nue, la jeune femme a bien évidemment piqué un fard et saisi un juge. Bilan de la mauvaise blague pour le farceur : matériel informatique saisi, caution de 12 500 dollars pour sa libération, et un jugement à venir. La vengeance est un plat qui se mange froid...

L'AMSTRAD CPC MORD TOUJOURS

Le célèbre crocodile revient en douce, grâce au travail des passionnés bénévoles du projet CPC-NG. Le cadençage du processeur fait un bond radical qui menace presque les utilisateurs de PC, puisqu'il saute carrément de 3,3 Mhz à 50 MHz ! Sa première amélioration depuis seulement 15 ans. Décidément, on n'arrête pas le progrès. Et tout ça en gardant la compatibilité avec les anciennes versions. En attendant que ce projet prometteur dépasse le stade alpha, c'est le moment de ressortir nos vieilles disquettes 3 pouces et de rejouer à Ghost'n Goblins ou Rick Dangerous. A propos, "NG" signifie "Next Generation" et pas "No Future" comme certains le disent (sinon ça aurait été NF (comment ça c'est une blague nulle ? (et les parenthèses ça se ferme (au fait on recherche les anciens rédacteurs du mythique magazine ACPC, sûrement SDF à présent, si vous en croisez dites-lui d'écrire au journal, merci !)))).

NIR UN HACKER

LA PHILOSOPHIE DU HACK

La philosophie du hack vu par la scène undergound. Le texte fondateur de l'éthique de centaines de hackers est-il encore d'actualité ?

L'éthique hacker au sens noble a pour fondement l'amour de la liberté. Certains sont allés encore plus loin pour émettre l'idée d'un droit fondamental de l'information à la libre diffusion. Le milieu underground s'est approprié ces idées, et en a déduit un concept encore plus extrême : les réseaux sont des espaces de pures informations, donc de libertés totales. Il est interdit de réglementer le réseau, de le soumettre à des lois, et bien sûr de protéger l'accès aux systèmes. D'ailleurs, si on appliquait des lois à cette jungle, elles ne sauraient être qu'au profit des technocrates qui nous dirigent, et au détriment des individus ordinaires.

Le Manifeste du Hacker a été publié il y a 15 ans par "The Mentor". Sa lecture montre bien l'esprit de pionnier, voire de colon, qui était celui des hackers à cette époque. Le réseau était vierge. Tout était à découvrir, tout était à créer. Le monde physique, méchant, injuste, rempli d'incompréhensions et dominé par l'argent, dégoûtait certains jeunes en quête d'un autre idéal. Cet idéal, ils pouvaient le fabriquer par eux-mêmes, dans une sorte de Nouveau Monde virtuel.

Depuis, les choses ont changé. Internet est devenu, pour sa majeure partie, la vitrine du monde réel. Commerces, publicités, services inter- et intra-entreprises, communications entre individus... L'espace de liberté possible a été conquis par le grand public et les sociétés, et s'interface de plus en plus avec toutes les activités du monde réel. De ce fait, il est inévitable (et indispensable) que des lois apparaissent pour le réglementer. D'autre part, le prix d'accès aux réseaux est devenu ridiculement bas grâce à Internet et à la mise en concurrence, ce qui balaye l'argument favori des phreakers : "nous utilisons un service déjà existant, sans payer ce qui pourrait être bon marché si ce n'était pas la propriété de gloutons profiteurs". Enfin, l'argument "d'accès à la connaissance", si prisé chez les pirates en herbe, ne tient plus. Il y a 15 ans, oui, c'était vrai ! Les gros systèmes étaient des UNIX ou des serveurs IBM propriétaires, dont les spécifications n'étaient accessibles qu'à certains initiés. Internet était réservé aux universités et aux grandes entreprises. Pour apprendre et pratiquer sur ces ordinateurs et ces réseaux, il fallait bien pirater. Mais de nos jours, on ne compte plus les UNIX gratuits, bien documentés, installables sur des ordinateurs personnels disponibles en supermarché...

Faut-il pour autant jeter aux orties ce Manifeste, ou considérer qu'il n'a qu'une valeur historique ? Non. Ce texte, que nous vous laissons découvrir ici, est toujours représentatif d'un certain mal-être des individus dans la société, et de la volonté toujours aussi forte d'évoluer dans un monde meilleur que chaque personne pourrait contribuer à créer. Que ce monde parfait soit l'Internet, on commence à en douter. Mais des espaces alternatifs de liberté s'organisent au sein même du grand réseau mondial. Les logiciels peer-to-peer et le réseau FreeNet en sont des exemples prometteurs. C'est peut-être vers là que la lutte doit se poursuivre...

LES LOIS ANTI-PIRATAGE EN FRANCE

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.

LE MANIFESTE DE "THE MENTOR"

LE SMART SPOOFING, C'EST DU BIDON !

Sur le papier, ça a l'air d'une révolution. Un article technique publié par la société Althes sur leur site web a été annoncé sur Internet comme "une découverte permettant de contourner tous les filtres basés sur l'adresse IP source". Traduction : les admins peuvent jeter à la poubelle leurs firewalls et leurs règles de contrôle d'accès (tcpwrappers, dns, serveur web...). Quand aux logs, ils ne sont plus fiables. Un vrai cauchemard. Pourtant, à la lecture, le lecteur averti comprend que c'est de la poudre aux yeux. La méthode proposée est déjà connue depuis des années, et en partie implémentée dans des logiciels publics comme hunt, ethercap ou dsniff. Elle présente des limitations intrinsèques et des pré-requis importants (il faut pouvoir contrôler localement une portion de réseau situé entre le serveur et la machine dont on souhaite usurper l'adresse IP ; sur Internet, il y a plus simple !). Mais inventer le spoofing IP intelligent, c'était un beau coup de pub pour cette société française.

WANTED

Plusieurs agences gouvernementales de renseignement, comme la très secrète DGSE chargée des missions offensives (espionnage) à l'étranger, viennent d'avouer des besoins cruciaux en informaticiens de haut niveau. Il semblerait qu'ils manquent de crédits pour attirer les meilleurs. Faute de compétences humaines, Big Brother ne serait donc pas (encore) français. (source: Le Monde)

33

C'est le nombre de magazines traitant du piratage informatique qui seront disponibles en kiosque en 2010, si la tendance actuelle se maintient. D'après mes calculs basés sur le graphique ci-contre, on observe une progression super-linéaire : dans deux ans, il y aura déjà 14 magazines différents ! On

JE SUIS UN HACKER, ENTREZ DANS MON MONDE...

Un autre s'est fait prendre aujourd'hui, c'est partout dans les journaux. "Scandale : Un adolescent arrêté pour crime informatique", "Arrestation d'un 'hacker' après le piratage d'une banque"... Satanés gosses, tous les mêmes.

Mais avez-vous, dans votre psychologie en trois pièce et votre profil technocratique de 1950, un jour pensé à regarder le monde derrière les yeux d'un hacker ? Ne vous êtes-vous jamais demandé ce qui l'avait fait agir, quelles forces l'avaient modelé ?

Je suis un hacker, entrez dans mon monde...

Le mien est un monde qui commence avec l'école... Je suis plus astucieux que la plupart des autres enfants, les conneries qu'ils m'apprennent me lassent...

Je suis au collège ou au lycée. J'ai écouté les professeurs expliquer pour la quinzième fois comment réduire une fraction. Je l'ai compris. "Non Mme Dubois, je ne peux pas montrer mon travail. Je l'ai fait dans ma tête" Satané gosse. Il l'a certainement copié. Tous les mêmes.

J'ai fait une découverte aujourd'hui. J'ai trouvé un ordinateur. Attends une minute, c'est cool. Ca fait ce que je veux. Si ça fait une erreur, c'est parce que je me suis planté.

Pas parce qu'il ne m'aime pas... Ni parce qu'il se sent menacé par moi... Ni parce qu'il pense que je suis un petit filou... Ni parce qu'il n'aime pas enseigner et qu'il ne devrait pas être là... Satanés gosses. Tout ce qu'il fait c'est jouer. Tous les mêmes.

Et alors c'est arrivé... une porte s'est ouverte sur le monde... Se précipitant à travers la ligne téléphonique comme de l'héroine dans les veines d'un accro, une impulsion électronique est envoyée, on recherche un refuge à l'incompétence quotidienne... un serveur est trouvé.

Vous vous répétez que nous sommes tous pareils... On a été nourris à la petite cuillère de bouffe pour bébé à l'école quand on avait faim d'un steak... Les fragments de viande que l'on nous a laissés étaient pré-machés et sans goût. On a été dominé par des sadiques ou ignoré par des apathiques. Les seuls qui avaient des choses à nous apprendre trouvèrent des élèves volontaires, mais ceux-ci sont comme des gouttes dans le désert.

C'est notre monde maintenant... Le monde de l'électron et de l'interrupteur, la beauté du baud. Nous utilisons un service déjà existant, sans payer ce qui pourrait être bon marché si ce n'était pas la propriété de gloutons profiteurs, et vous nous appelez criminels. Nous explorons... et vous nous appelez criminels. Nous recherchons la connaissance... et vous nous appelez criminels. Nous existons sans couleur de peau, sans nationalité, sans dogme religieux... et vous nous appelez criminels. Vous construisez des bombes atomiques, vous financez les guerres, vous ne punissez pas les patrons de la mafia aux riches avocats, vous assassinez et trichez, vous manipulez et nous mentez en essayant de nous faire croire que c'est pour notre propre bien-être, et nous sommes encore des criminels.

Oui, je suis un criminel. Mon crime est celui de la curiosité. Mon crime est celui de juger les gens par ce qu'ils pensent et disent, pas selon leur apparence. Mon crime est de vous surpasser, quelque chose que vous ne me pardonnerez jamais.

Je suis un hacker, et ceci est mon manifeste. Vous pouvez arrêter cet individu, mais vous ne pouvez pas tous nous arrêter... après tout, nous sommes tous les mêmes.

ECRIT LE 8 JANVIER 1986
PAR THE MENTOR
TRADUIT PAR NEURALIEN
LE 8 SEPTEMBRE 1994

HACKER, CRACKER, WHITE HAT, SCRIPT-KIDDIE, LAMERZ, COWBOY, CARDER

Mais que veulent dire exactement tous ces mots ? Pour ceux qui débarquent, voici les définitions indispensables. Elle vous donneront une première vision des différents acteurs de la grande scène du "hacking" et de l'underground.

Le terme de hacker est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatiques aiment à penser qu'ils ont été attaqués par des pirates chevronnées ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour créer une faille dans leur système.

Le terme hacker a eu plus d'une signification depuis son apparition à la fin des années 50. A l'origine ce nom désignait d'une façon méliorative les programmeurs émérites, puis il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.

C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.

Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques.

LES DIFFÉRENTS TYPES DE PIRATES

En réalité il existe de nombreux types d'"attaquants" catégorisés selon leur expérience et selon leurs motivations :

LES WHITE HAT HACKERS, hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple.

LES BLACK HAT HACKERS, plus couramment appelés **pirates** (ou appelés également **crackers** par extension du terme), sont des personnes s'introduisant dans les systèmes informatiques dans un but nuisible.

LES SCRIPT KIDDIES (traduisez gamins du script, parfois également surnommés **crashers, lamers** ou encore **packet monkeys,** soit les singes des paquets réseau) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.

LES PHREAKERS sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de les utiliser gratuitement grâce à des circuits électroniques (qualifiées de box, comme la blue box, la violet box, ...) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement.

LES CARDERS s'attaquent principalement aux systèmes de cartes bancaires pour en comprendre le fonctionnement et en exploiter les failles

LES CRACKERS ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants.

LES HACKTIVISTES (contraction de hackers et activistes que l'on peut traduire en cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement de **underground**).

Dans la réalité ce type de distinction n'est bien évidemment pas aussi nette, dans la mesure où certains (white hat) hackers ont parfois été crackers (black hat hackers) auparavant et parfois inversement. Les habitués des listes de diffusion et des forums voient souvent des sujets à propos de la différence qu'il convient de faire entre pirate et hacker. Le terme de troll est généralement utilisé pour désigner les sujets délicats déclenchant un engouement dans les réponses.

LA CULTURE DU "Z"

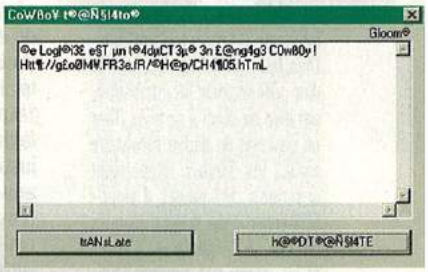
Le Z symbolise le pluriel. Voici un certain nombre de définitions issues du milieu underground, et maintenant pratiquement banalisées :

WAREZ : piratage de logiciels
APPZ (applications + warez) : piratage d'applications
GAMEZ (games + warez) : piratage de jeux vidéos
SERIALZ (serials + warez) : il s'agit de numéros de série permettant d'enregistrer illégalement des copies de logiciels commerciaux
CRACKZ (cracks + warez) : ce sont des programmes écrits par des crackers, destinés à supprimer de manière automatique les système de protection contre la copie des applications commerciales.

LE LANGAGE "COWBOY"

Les adeptes de la communication en temps réel (IRC, chat) se sont sûrement déjà retrouvés engagés dans une discussion avec un utilisateur s'exprimant dans une langue peu commune, dans laquelle les voyelles sont remplacées par des chiffres. Je ne parle pas ici des abréviations chères aux utilisateurs de SMS. Ce langage, particulièrement utilisé dans le milieu des script-kiddies (les vrais hackers ne l'utilisent plus), se nomme le langage "c0wb0y". Il consiste à remplacer certaines lettres (la plupart du temps des voyelles) par des chiffres. Voici quelques substitutions possibles :

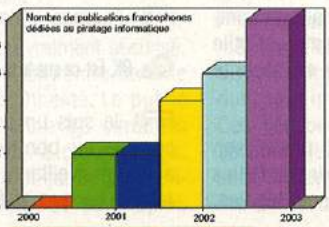
E=3
A=4
B=8
O=0
I=1
T=7



Il en existe beaucoup d'autres, faisant même intervenir des caractères spéciaux, et alternant minuscules et majuscules.

Des programmes existent pour traduire du langage c0wb0y en français et vice-versa (voir notre photo d'écran d'un "c0wb0y translator").

Voici ce que cela peut donner sur deux mots de la vie courante :
Elite = eleet = 31337
Anticonstitutionnellement = 4nT1c0Ns7|Tut10NnEIL3m3nT



dirait bien qu'il y a un marché à prendre : je crois que c'est le moment de sortir un Pirat'Z hors-série avec un CD du Pirat'Z (un peu bidon mais en bonus on mettrait une petite vidéo érotique pour faire vendre). Et puis, on pourrait vendre par correspondance un bouquin exceptionnel ultra exclusif sur la scène Pirat'Z. Ah zut, trop tard, on me dit que tout ça a déjà été fait. Je vous donne donc rendez-vous dans notre prochain numéro... si vous réussissez l'exploit de ne pas vous embrouiller.

HACKER PRO
VOTRE FUTU

Il y a des débouchés pour les passionnés du piratage. Devenir hacker professionnel, c'est possible ! Quelles sont les qualités qu'il faut posséder pour y parvenir ? Interview vérité.

Les hackers passionnés se retrouvent tous sur Internet, sur le réseau de chat IRC. Certains sont hackers par hobby, le soir quand ils rentrent chez eux. Mais on remarque que d'autres sont connectés toute la journée. Et pour cause : c'est leur job !

Qui recrute officiellement des hackers ? Tout d'abord, des sociétés de sécurité informatique. Elles sont principalement américaines pour le moment, mais certaines ont des filiales en France. ISS et Snosoft sont des pionniers dans ce domaine. D'autre part, de grosses multinationales qui veulent bénéficier d'une expertise technique de haut niveau en interne et recrutent à cet effet des "ethical hackers" (hackers éthiques). L'exemple le plus frappant est celui d'IBM.

En quoi consiste leur métier ? Le groupe de white hats de X-Force, au sein de la société de sécurité ISS, réalise des tests d'intrusion sur leurs entreprises clientes. Ils travaillent également à l'amélioration de leurs logiciels : un scanner automatisé de vulnérabilités et un détecteur d'intrusion. Ils se font connaître en menant des recherches en sécurité informatique et en en publiant les résultats sur Internet. KF, un hacker réputé, est employé par Snosoft pour chercher des failles de sécurité dans des logiciels commerciaux ou open-source et les publier au nom de sa compagnie sur BugTraq (la liste de diffusion de référence des experts en sécurité informatique). KF code et diffuse également les "exploits" qui peuvent permettre à un pirate d'utiliser ses failles pour rentrer dans les systèmes vulnérables. La justification est que ces exploits peuvent servir aussi aux administrateurs pour vérifier s'ils ont bien appliqué tous les correctifs de securité. On peut donc mener une activité fun de vrai hacker, avec la bénédiction et la couverture de son entreprise !

Thor, un hacker du groupe Hammer Of God, a été interviewé par notre ami le hacker français Fozzy. L'interview a été réalisée l'année dernière au DEFCON, la plus grande réunion de hackers au monde, à Las Vegas. Nous avons obtenu l'autorisation de la publier dans Pirat'Z. Les réponses apportées par cette interview sont très intéressantes. Faut-il forcément avoir été "black hat" pour faire un bon "white hat" ? Peut-on s'éclater à faire ce que l'on aime sans pour autant sombrer dans l'illégalité ? Quel type d'hacktivisme est utile et moral ? Et aussi, que penser du niveau de sécurité de nos systèmes Windows ?

Thor est un hacker professionnel. Il passe son temps à développer des logiciels, à chercher des failles de securité, et à les corriger. Ses activités sont légales, et il gagne très bien sa vie grâce à elles. Thor est connu pour ses nombreux articles publiés sur le site de référence de la sécurité informatique securityfocus.com. Il adore chercher de nouvelles failles et révéler au monde tout ce qu'il pourrait faire grâce à elles, si seulement il le voulait...

A la fin de sa première conférence au DEFCON, le responsable sécurité d'une banque anglaise était venu le voir, affolé, pour lui demander comment se protéger d'un des trous de sécurité qu'il avait découvert. Sa réponse fut: "pour l'instant il n'y a pas de moyen efficace à 100%, à part vous assurer que tous vos utilisateurs ont des mots de passe très forts, auquel cas il faudra trois mois à un attaquant pour les craquer". Pas de bol, les systèmes bancaires en question possèdent plus de 10000 utilisateurs...

"SI TU VEUX FAIRE PARTIE DES MEILLEURS, TU DOIS ÊTRE CAPABLE DE CRACKER DES SYSTÈMES"

Q: Peux-tu nous faire une présentation de toi et de ce que tu fais ?

R: Dans la vraie vie, je m'appelle Timoth Mullen. Je conçois des logiciels et des procédures de gestion sécurisés ("accounting software"). A AnchorIS, l'entreprise dans laquelle je travaille, nous vendons un système sécurisé complet de ce type. De plus, je suis membre fondateur d'un groupe de sécurité appelé "Hammer of God" (le "Marteau de Dieu"). Nous avons lancé cela il y a quelques années. C'est une sorte de rassemblement de gens ayant des compétences techniques et disposés à les partager. Nous avons de nombreux membres qui travaillent dans de grandes compagnies... par exemple, on a des gens de Microsoft qui utilisent le site "Hammer of God" comme une plate-forme de lancement pour leur propre developpement, des trucs comme ça. Nous offrons un e-mail anonyme, nous offrons des ressources, bref, un endroit où réaliser des choses qu'ils ne pourraient pas faire autrement. Voilà, c'est vraiment ça "Hammer of God": un refuge où les gens peuvent venir et accomplir ce qu'ils veulent vraiment faire, quand ils sont limités par une corporation.

Q: Pourquoi avoir choisi ce surnom, Thor ?

R: Pourquoi ? Ha... Heu... C'est comme ça, c'est tout !

Q: OK. Est-ce que tu te définis comme un "hacker", et quel type de hacker ?

R: Je suis un pur hacker, au sens premier du mot, comme au bon vieux temps. Je ne commet aucune action malveillante, et je condamne quiconque le ferait. Je fais ce que je fais parce que j'adore tout ça, c'est

LINUX PLUS VULNÉRABLE QUE WINDOWS

Aberdeen Group, entreprise de conseil, a publié une étude qui met en relief les problèmes de sécurité qui seraient plus nombreux sur Linux que sur Windows. Pour les dix premiers mois de 2002, les produits Microsoft n'ont pas reçu d'alertes du CERT concernant de nouveaux virus ou chevaux de Troie alors que Linux en a reçu deux. Il faut d'ailleurs souligner que mis à part Microsoft, tous les systèmes d'exploitation, à commencer par Mac OS X (4 alertes) sont plus vulnérables cette année que l'an passé. Microsoft, contre les idées reçues, ne serait donc pas le pire système en matière de failles de sécurité. Les logiciels libres, eux, seraient aussi sensibles que les autres systèmes aux virus. Ce sont là des opinions courageuses qui méritaient d'être soulignées !

PERPÉTE POUR LES HACKERS

Si la proposition de loi instaurant un département de la sécurité intérieure est acceptée aux Etats-Unis, les pirates informatiques, et plus généralement les internautes, ont bien du souci à se faire. Dans un contexte de dérive sécuritaire aiguë, les pirates risqueraient désormais des peines d'emprisonnement à vie, si leurs attaques ont mis en danger la vie d'autrui et les internautes seraient étroitement surveillés. Les associations de défense de la vie privée crient au scandale et craignent que des données personnelles soient collectées sur le dos des internautes. Le texte va loin, puisqu'il prévoit que les FAI pourraient plus facilement faire part d'activité suspectes se déroulant sur leurs réseaux et transmettre les données personnelles de certains clients sans craindre un procès. Ce texte doit encore être examiné par le Sénat... espérons que les sénateurs arrêteront le délire avant qu'il ne soit trop tard !

FESSIONNEL : UR METIER ?

comme un grand puzzle. J'aime remettre les pièces les unes à côté des autres, et découvrir quelles sont les vulnérabilités afin de pouvoir protéger les gens, pas pour les exploiter, arrêter des serveurs ou faire des choses comme ça. Celui qui fait ça a tout faux. Je m'explique: ce n'est pas parce que vous avez des compétences pour pénétrer dans les systèmes que vous devez le faire. Si vous êtes bon au tir au pigeon, ça ne veut pas dire que vous devez sortir dans la rue pour dégommer les passants. Ce n'est pas une bonne chose.
Je me définis donc comme un vrai hacker (NDT: "I am... you know... a TRUE HACKER") , pas un cracker ou une merde dans ce genre-là, ni un script-kiddie. Je ne suis pas d'accord avec les actions qui coûtent de l'argent aux autres, qui corrompent des serveurs, etc.

Q: Que penses-tu de l'hacktivisme, ou plus exactement du fait de cracker les sites web illégaux, ou ceux de compagnies qui ne respectent pas les droits de l'homme, par exemple ?

R: Ce que je pense des personnes qui crackent des sites web qui sont despotiques, racistes, et caetera ? Et bien, ça reste illégal. Je suis contre. Le racisme, l'enfance maltraitée, la pédophilie, je trouve ça horrible. Tu vois, j'ai des enfants, et si quoi que ce soit devait les menacer, je ferais tout ce qui est en mon pouvoir pour les protéger. Mais, malgré un but généreux, même si ça pourrait être une bonne chose, quand vous leur faites ça vous les privez de leur droit à la liberté, de leur droit à la parole, de leur droit à leurs croyances. Et je pense que même s'ils violent, tuent et mangent des animaux familiers, si vous piratez leur site, vous ne valez pas mieux qu'eux. Vous leur imposez vos convictions, exactement comme ils essaient de le faire avec vous, et au final vous devenez comme eux.

(...)

Q: Tu nous as parlé des défauts de Windows. Il n'y a pas seulement des problèmes bénins portant sur une partie du code, pouvant être résolus facilement, mais aussi de problèmes structuraux plus globaux. Peut-être que Windows n'est pas conçu pour la sécurité ?

R: En fait, Windows peut être rendu vraiment sécurisé. C'est comme n'importe quoi d'autre, on rentre dans le débat de la sécurité contre la fonctionnalité. Le public qui achète les produits de Microsoft exige certaines fonctionnalités. Ils veulent pouvoir faire ça, ça et ça. Microsoft leur permet de faire ça, ça et ça. Si la sécurité devient alors un problème, ça doit être traité après coup dans de nombreux cas. Je veux dire: la fonctionnalité est prioritaire, on se place d'un point de vue économique. De ce fait, si vous voulez mettre en place des applications critiques avec les produits de Microsoft, il vous suffit de bien former l'équipe que vous mettez dessus.
Malheureusement, c'est extrêmement facile d'installer un Windows 2000 avec un serveur SQL, et de mettre du contenu sur Internet. C'est génial pour les petites entreprises familiales, par exemple. Tu vois, avec un investissement relativement faible ils arrivent à être présents sur le marché mondial. Il n'y a pas si longtemps c'était une aventure très couteuse. Mais par la même occasion, ils introduisent dans leur modèle économique des risques de sécurité dont ils n'ont même pas conscience.
Mais... c'est ça faire des affaires ! Je m'explique: si tu ouvres une boutique dans un quartier chaud de la ville pour faire plus de chiffre d'affaire, tu dois mener une recherche pour trouver le dispositif de sécurité le plus adapté. C'est comme partout, tu dois savoir ce que tu fais ou sinon t'auras des ennuis.
Je ne dirai donc pas que les produits de Microsoft ne sont pas sécurisés; je dirai que dans ce cas précis, ils facilitent la récupération des données d'authentification des utilisateurs. Mais, tu sais, on pourrait tout simplement stopper NTLM. Il y a des moyens pour le faire. Ou alors, mettre la version 2 de NTLM qui utilise des clés d'encryption de 128 bits: il faudrait alors attendre jusqu'à la fin du millénaire pour cracker un mot de passe. On peut donc se protéger efficacement.

Q: Parlons un peu des versions personnelles de Windows, comme 95, 98, et Millenium. Ces systèmes d'exploitation sont utilisés en interne dans de nombreuses entreprises pour écrire des rapports, lire le courrier électronique, etc... Plutôt que de s'attaquer aux sites accessibles directement depuis l'internet, qui sont bien protégés, un pirate pourrait envoyer un cheval de troie par mail directement à une personne à l'intérieur de l'entreprise, en profitant des nombreux bugs de ces versions de Windows. Ceci lui donnerait alors accès à tout le réseau interne, souvent mal sécurisé. Penses-tu que Windows soit un point faible dans la sécurité d'un réseau d'entreprise ?

R: Si une compagnie se sent concernée par la sécurité, alors elle serait stupide de charger Windows 95, 98, ou n'importe quelle version personnelle de ce produit pour une utilisation professionnelle en entreprise. Ces versions de Windows n'ont absolument aucune sécurité. Revenons à l'exemple de la boutique. Si je me sens réellement concerné par la sécurité, je ne vais pas me contenter d'un verrou sur ma porte, que je pourrai

12

SUPER RÉPRESSION POUR CYBERDISSIDENT

Lee Chi Quang, professeur d'informatique à Hanoi (Vietnam) âgé de 32 ans, a été condamné à 4 ans de prison et trois ans de résidence surveillée pour " délit d'opposition à l'Etat ", à l'issue d'un procès expéditif (moins de trois heures). Le dissident avait pour seul tort d'avoir publié sur Internet des articles critiques à l'égard du régime communiste. Il semble que la politique du régime vietnamien s'aligne sur celle du gouvernement chinois en matière de lutte contre la liberté d'expression sur Internet. Un modèle pourtant tristement célèbre.

NAPSTER, DERNIER SOUFFLE ?

Fermé par la justice en juillet 2001, le site de téléchargement de musique Napster, pionner du Web, pourrait ressusciter, puisqu'il a trouvé un repreneur. Il s'agit de Roxio Inc, le fameux propriétaire d'Easy Creator, logiciel de gravure pour CD. Le tribunal des faillites du Delaware doit toutefois se prononcer sur cette candidature avant qu'elle ne soit acceptée. Roxio propose 5 millions de dollars et 100 000 de ses actions pour un tel rachat, mais souhaite évidemment récupérer la marque uniquement et non les passifs judiciaires de l'entreprise. Napster parviendra-t-il enfin à renaître de ses cendres ?

SORCELLERIE SUR LE NET

La Warner, producteur de " Harry Potter 2" a du souci à se faire : le film, annoncé comme une bombe au box-office, était disponible sur le Net avant même la sortie officielle américaine ! Ces copies pirates, même si elles sont en général de piètre qualité, auraient été téléchargées plusieurs milliers de fois pour le seul week-end qui a suivi la sortie du film pour enfants le plus célèbre au monde. Les français ont donc pu assouvir leur " pottermania " en toute tranquillité...

LE PIRATAGE DE CD FAIT DES RAVAGES AU MEXIQUE...

... à tel point que la Cour Suprême, située au cœur de Mexico City, aurait déménagé par sa faute de ses locaux, auprès desquels les ventes sauvages ont pris une ampleur jamais observée. C'est du moins ce que prétend la puissante RIAA, Recording Industry Association of America, un brin parano. Ce serait à cause du bruit excessif des sonos crachant leur musique à l'extérieur que le plus haut tribunal du pays s'en serait allé, à la recherche de la tranquillité d'un bâtiment disposant de fenêtres aux doubles. Et la RIAA regrette que la Cour suprême mexicaine, plutôt que de lutter contre le problème du piratage, se contente de faire l'autruche en déménageant dans un quartier plus tranquille. Pour vivre heureux, vivons cachés...

ouvrir facilement avec une carte de crédit ou en enfonçant la porte avec 15 kilos de pression. Si j'ai des objets de valeur à l'intérieur, je dois avoir des outils adaptés à leur valeur pour les protéger. Ce que je veux dire, c'est que je ne vais pas protéger 1 million de dollar de diamants par une alarme qui fait "ding dong" quand on ouvre la porte.

C'est la même chose avec les systèmes d'exploitation dans les entreprises. Si, juste pour économiser de l'argent, notre compagnie choisit de déployer partout une installation par défaut de Windows 98, ils se plantent completement. Tu sais, Cisco a toujours une machine avec 98 dessus, je trouve ça étonnant, c'est ridicule. Mais je crois qu'ils vont continuer à le faire. Dans ce cas oui, en effet, cela introduit d'énormes trous de sécurité. Tu ne peux pas gérer les politiques de domaines, tu ne peux pas contrôler les accès, tu ne peux rien faire. C'est donc une grosse erreur.

Les gens doivent rechercher les bonnes configurations des ordinateurs et les bonnes configurations de sécurité exactement comme ils recherchent les modèles économiques quand ils se lancent dans une entreprise. Ils analysent le marché visé, les produits qu'ils proposent et leur stratégie de marketing, comment ils vont les produire, avec quel matériel, tout. Et puis... ils mettent Windows 98 sur toutes leurs machines ! Voilà le problème. De nos jours, le logiciel utilisé et la manière dont il va être sécurisé doit devenir une partie intégrante du modèle économique.

Q: Fais-tu de l'audit pour des entreprises extérieures ?

R: On nous a demandé de faire quelques audits via AnchorIS. La gestion des comptes est un domaine crucial pour les grosses entreprises. Pourtant, la sécurité des procédures de gestion est très souvent confiée au niveau applicatif uniquement ! A l'inverse, nous nous plaçons sur une toile de fond sécurisée, nous avons nos propres serveurs, nos propres systèmes d'exploitation, nous installons tout nous-mêmes, nous avons écrit le code, nous apportons tout. Voilà ce que fait AnchorIS. Pour ce qui est des audits, on nous a effectivement demandé quelques tests d'intrusion, des trucs comme ça, mais ce n'est pas notre spécialité. Personnellement, je l'ai déjà fait plusieurs fois, mais ce n'est pas vers cela que notre entreprise s'oriente. Nous allons vendre des logiciels.

Q: Dernière question: penses-tu que pour être un expert dans le domaine de la sécurité informatique, il faut avoir été auparavant un "black hat" ?

R: Tu sais, même le mot "black hat" a différentes connotations. C'est clair, il faut pénétrer par effraction dans des systèmes, il faut les hacker, mais tu peux rentrer dans tes propres machines, ou dans celles du labo d'à côté, dans celles de tes amis... Il n'y a aucun besoin de se promener sur des machines prises au hasard connectées à un modem cable, et de détruire leurs données. Quand ça devient malveillant, tu n'as pas besoin de continuer à agir. Mais si tu veux faire partie des meilleurs, tu dois être capable de cracker des systèmes. Tu dois avoir envie de le faire. Ce que je crois, c'est que la sécurité informatique est un ART, et pour percer dans ce domaine il ne suffit pas d'apprendre des choses. Il faut vouloir vraiment y arriver, et il faut avoir un certain talent. Mais je ne pense pas qu'il faille se lancer dans des activités illégales pour être bon, il faut juste... le VOULOIR ! (il rit)

Q: Merci beaucoup.

Anonymat DO IT!

ENVOYER UN FAKE MAIL FACILEMENT

Votre patron vient de recevoir un message d'insultes provenant de votre adresse e-mail personnelle. Comment le convaincre que vous n'y êtes pour rien ? Montrez-lui cet article, qui démontre combien il est simple de se faire passer pour quelqu'un d'autre sur Internet.

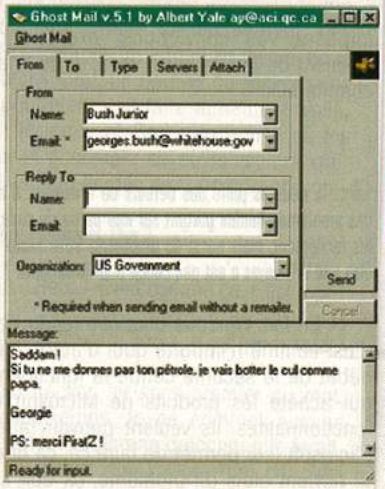
Le protocole de messagerie électronique utilisé sur Internet a été inventé à la base pour que les chercheurs universitaires puissent se communiquer facilement leurs résultats. À l'époque, personne ne prévoyait l'ampleur que le réseau des réseaux allait prendre. La menace des pirates informatiques n'était pas au centre des préoccupations. De ce fait, le protocole est intrinsèquement non sécurisé : il n'y a pas d'authentification (d'où la possibilité de prendre l'identité de quelqu'un d'autre), ni de chiffrement des données (donc possibilité de lire les messages quand ils transitent sur le réseau).

Le protocole, appelé SMTP, permet à n'importe qui d'envoyer un message en mettant n'importe quelle autre personne en adresse d'émetteur ! Vous connaissez peut-être déjà la bonne vieille technique du mail anonyme par "telnet" : on se connecte en telnet sur le port 25 (SMTP) d'un serveur de mail, et on rentre des commandes d'envoi d'email :

```
telnet serveur.de.mail 25
HELO host
MAIL FROM: lamer@pipo.com
RCPT TO: victime@victime.com
DATA
From: "un leet hacker"
<lamer@pipo.com>
To: "toto" <victime@victime.com>
[retour chariot, puis le texte du message, puis un "." sur la dernière ligne]
```

Par exemple, si vous utilisez le FAI Free, un serveur de mail valide pourra être smtp.free.fr. Les spammers professionnels cherchent des serveurs de mail mal configurés, autres que celui de leur FAI, qu'ils pourront utiliser pour relayer leurs messages. Le top du top, pour le pirate comme pour le spammeur, c'est de trouver un serveur de messagerie buggué qui permet de cacher ou de modifier l'adresse IP d'origine du message. L'émetteur du message sera alors virtuellement impossible à retrouver !

Cette technique d'envoi de message à la main par telnet est assez fastidieuse. Elle a été automatisée dans un petit logiciel, qui s'appelle Ghost Mail, qu'on peut trouver facilement



LA LETTRE AU PERE NOEL D'UN 1337 HACKERZ ;)

Hacking is not a crime ! Le père noël ne vous tiendra donc pas rigueur d'avoir supprimé toutes les mp3 de Britney de MissNeuneu ou d'avoir défacé la page d'accueil d'un célèbre site d'un fabricant de poupées en plastique qui fournit LE modèle de beauté de la société américaine.

De toute façon le père noël se fiche pas mal de ce que vous avez fait ou pas fait vu qu'il fonctionne plus en fonction de la bourse de vos parents ou de la générosité du Comité d'Entreprise.

Pour vous aider à préparer votre liste de noël dans l'esprit "pur3 1337 hax05", nous avons préparé une liste des cadeaux qui vous seront indispensables pour l'année prochaine... Tous propos parodiques sont à prendre au second degré bien sûr ;)

LINUX 4 L33T ET BONNES CHOSES POUR LA TÊTE :

Tout d'abord, pour pouvoir bénéficier de tout le respect de la part de vos futurs congénères, il vous faut des bouquins. Nous allons commencer par le commencement : l'installation de linux avec la version imprimée du guide d'install LFS (linux from scratch - linuxfromscratch.org). Rassurez-vous, vous n'aurez pas à galérer pour installer linux : ce bouquin n'est là que pour impressionner (le hacker est souvent fier et vantard je vous rappelle ;). Pour installer linux, vous commanderez la Mandrake 9.0 en 3 CD que vous cacherez dans un endroit sûr (la chambre de votre petite soeur ?). Prenez également quelques bouquins de l'éditeur O'Reilly sur les réseaux et la sécurité, ça vous permettra de faire le gros mac et accessoirement d'assouvir la soif de connaissance que tout hacker digne de ce nom se doit de revendiquer.

HARDWARE[Z] :

Il vous faut un instrument à la hauteur de votre talent pour pratiquer votre art... Vous allez avoir besoin d'un mini portable. Pour à peine 3000 euros (100 années d'argent de poche) sur le site www.sony.fr vous pouvez accéder au VAIO PCG-C1MHP de Sony dont les mensurations de rêve ne manqueront pas de vous séduire : 249 mm de longueur x 28,5 mm de hauteur x 152,5 mm de profondeur à cacher dans votre long manteau de cowboyz duelliste des temps électroniques modernes.

Bien entendu, il va vous falloir une carte wireless 802.11b pour vos promenades quotidiennes car le hacker moderne n'est plus le stéréotype du jeune boutoneux au teint blafard : le war driving a changé sa vie !!! Pour environ 160 euros port compris une bonne vieille carte Orinoco Gold vous sera livrée par www.wirelesscentral.net et vous permettra de découvrir les entreprises qui laissent leur LAN accessible par l'intermédiaire des réseaux sans fil.

R33BLZ

Tout hacker qui se respecte est un rebelle de la société capitaliste qui vend son âme sur Internet (la société, pas le rebelle). Pour dénoncer cela, le site www.unamerican.com vend des tee-shirt et des stickers ! (qui a dit que c'était contradictoire ? ;)

Pour être à fond dans le stylez, imaginez votre ordinateur recouvert de citations philosophiques et de phrases chocs telles :

'fuck work', 'hackerz n33d s3x 2' ou 'make love not work'.

Vous apprécierez la profondeur des nombreux modèles proposés ainsi que la fraîcheur de l'humour sous-jacent qui sera du plus bel effet sur la nouvelle robe de chambre de pépé !

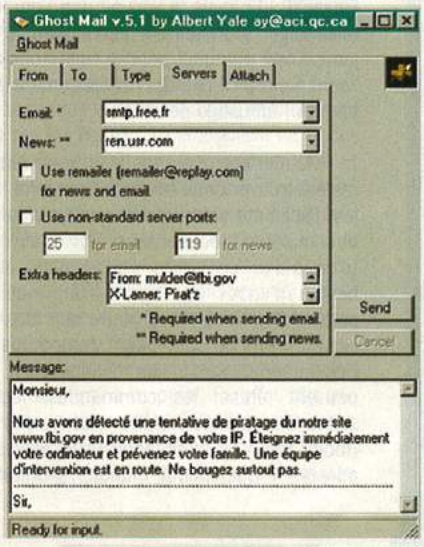
LES TCHÉTCHÈNES PIRATÉS PAR LE KGB

Les séparatistes tchétchènes accusent les services de sécurité russes -le fameux FSB- d'avoir piraté deux sites Internet où les rebelles puisent leurs informations. Conjointement à la prise d'otages qui a eu lieu dans un théâtre à Moscou, les sites www.chechen-press.info et www.kavkaz.org ont été attaqués par des pirates informatiques. Kavkaz.org est un site enregistré aux Etats-Unis et dirigé par Movladi Ougoudov, un ancien ministre tchétchène en exil, qui s'est déclaré " surpris que les services spéciaux russes puissent opérer aussi librement sur le territoire américain ". Le FSB s'est refusé à tout commentaire ; son porte-parole, Andrei Larouchine, s'est contenté d'un laconique : " ils ont l'habitude de mentir ". L'attaque a été particulièrement bien menée, puisque pour le cas de Kavkaz.org, l'enregistrement du nom de domaine a été modifié contre la volonté de l'administrateur du site, ce qui a conduit à une fermeture du site. Une nouvelle " bavure " à mettre sur le compte du FSB, dont l'ancien dirigeant n'est autre que... Vladimir Poutine lui-même !

Pour se protéger de cette attaque, il faut afficher tous les en-têtes (headers) des messages que l'on reçoit, et en vérifier la cohérence. Les en-têtes retracent le chemin du message, depuis son expéditeur jusqu'au destinataire, à travers les différents serveurs SMTP servant de relais. Les adresses IP et les noms de machines sont mentionnés, ainsi que les dates et heures de passage. Par exemple, un message envoyé depuis une adresse IP d'AOL à travers un serveur SMTP américain peut difficilement venir de votre copine qui utilise Wanadoo. Mais on voit sur une de nos photos d'écran que Ghost Mail permet de rajouter des headers dans le mail, histoire de brouiller les pistes...

en cherchant sur google. Les plus de ce programme : il peut envoyer des pièces jointes, des messages au format HTML, et on peut aussi l'utiliser pour poster anonymement sur les newsgroup ! L'utilisation de cet outil est à la portée de tous, même si l'on ne comprend pas bien l'anglais. Il suffit de donner les noms et adresses de la fausse source, du destinataire, et de spécifier le serveur de mail que l'on souhaite utiliser. Puis entrer le texte du message, rajouter la pièce jointe éventuelle dans l'onglet "Attach", et cliquer sur "Send". Un logiciel puissant, qui démontre parfaitement les faiblesses et les dangers du protocole de messagerie d'Internet.

La conclusion à tirer de cette démonstration, c'est qu'un e-mail important qui n'est pas signé cryptographiquement (par PGP par exemple) ne doit jamais être pris au sérieux. Passez un coup de fil à la personne concernée pour confirmation avant de vous lancer dans des actions inconsidérées !



LES BOARDS FXP : LA GRANDE DISTRIB

ATTENTION !
Il est fait allusion au scanning dans cet article, nous vous déconseillons fortement de vous y essayer ! Les FAI voient généralement cette activité d'un très mauvais oeil (car bien que ne faisant aucun dommage, elle est considérée comme la première étape avant une tentative de hack). Donc si vous ne voulez pas avoir de problèmes (avec votre FAI comme avec la justice), ne scannez pas ! Et, évidemment, ne téléchargez rien d'illégal, rappelons-le pour nos nouveaux lecteurs ;)

Dans les quatre premiers numéros de Pirat'gamez, le prédécesseur de Pirat'Z, nous vous avions présenté les principales facettes du net pirate : le web, le Peer-to-Peer (P2P), les News, l'IRC et les groupes pirates. Dans cette dernière partie, il était fait mention des boards FXP, et c'est le sujet qui va nous intéresser aujourd'hui : il s'agit en effet d'un côté de la scène underground à la fois méconnu du public, et pourtant très développé et accessible à n'importe qui ! Nous avons enquêté sur le sujet, afin de vous en dévoiler le plus possible sur ces fameux boards...

FXP KÉZAKO ?

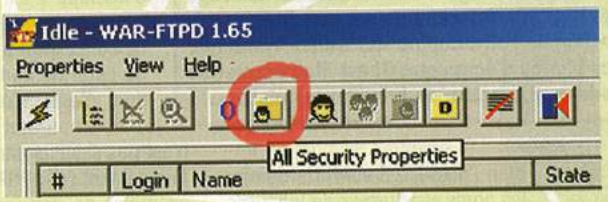
Petit rappel pour les cancres qui ont déjà oublié la leçon du n°4 (ou pire, qui étaient absents, n'oubliez pas d'envoyer un mot d'excuse des parents au journal d'ailleurs) : FXP signifie " File eXchange Protocol ", et est donc une déformation de FTP (" File Transfer Protocol "). Et en clair ? Au lieu de transférer des données d'un serveur FTP vers votre ordinateur, en utilisant le FXP vous pouvez échanger les données entre deux serveurs FTP. En réalité, le FXP n'est que l'utilisation judicieuse de commandes du protocole FTP, il n'y a donc rien de magique là-dedans.

Vous voulez faire du FXP ? La première étape sera d'installer un logiciel (client) FTP capable de gérer le transfert FXP (de serveur à serveur). En effet, beaucoup de logiciels ne sont prévus que pour vous permettre de télécharger / uploader sur un serveur FTP, et n'incluent pas dans leur interface la possibilité de se connecter à plusieurs serveurs. Le plus fameux et le plus puissant des clients pour le FXP sous Windows est FlashFXP [1], mais la version que l'on peut télécharger gratuitement est limitée à 30 jours. C'est pourquoi pour la suite nous utilisons SmartFTP [2], qui est totalement gratuit pour un usage personnel.

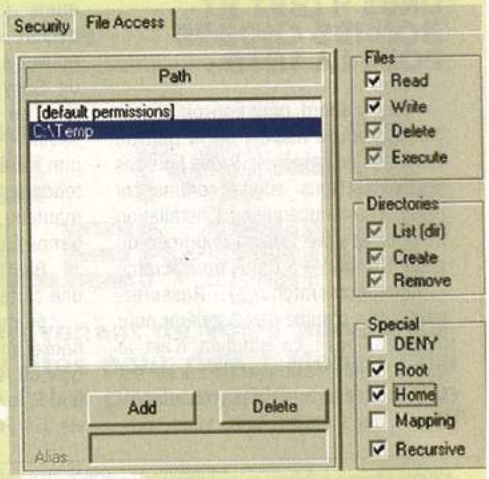
Maintenant que vous avez votre client, reste à trouver deux serveurs pour faire joujou. Facile me direz-vous, il existe sur le net une multitude de serveurs FTP anonymes (c'est-à-dire en accès public, sans avoir besoin d'entrer un login et un mot de passe). Oui, MAIS : il se trouve que tous les serveurs FTP ne sont pas " compatibles " FXP. En effet, selon leur configuration, ils peuvent refuser les commandes nécessaires au transfert entre deux serveurs (mode PASV ou commande PORT vers une adresse IP quelconque interdits, problèmes de compatibilité entre serveurs). C'est aujourd'hui d'autant plus le cas que les boîtes commercialisant des serveurs FTP se sont rendu compte que le transfert de FTP à FTP pouvait être exploité à des fins peu recommandables (ce dont on va parler tout à l'heure), et ont par défaut désactivé cette possibilité. Ici je ne veux de toute manière que vous montrer le principe, donc inutile d'aller chercher des serveurs bien loin, le mieux est encore de tester sur les vôtres.Ben oui, je préfère ne pas vous donner des adresses de serveurs dispos sur le net, car tels que je vous connais vous y mettriez un sacré bronx. Comme serveur FTP, nous voulons juste faire un test, alors allez télécharger WarFTPd sur [4]. Ce n'est pas la dernière version, mais encore une fois, c'est juste pour la démo.

Créez des répertoires C:\Temp\Serveur1et C:\Temp\Serveur2. Copiez-y le fichier exécutable téléchargé, et lancez-le : divers fichiers sont décompressés, dont " war-ftpd.exe ", que vous allez lancer. Cliquez sur le OK de la bannière, puis dans la partie " IP number and port " à droite, dans le second serveur, remplacez 21 par 22. Ensuite, pour les deux serveurs, faites les opérations suivantes :

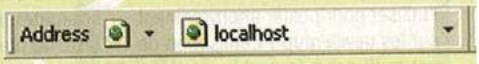
- décochez la case " No anonymous logins " en haut à droite
- cliquez en haut sur l'icône " All Security Properties " :



- une fenêtre apparaît, avec en haut à gauche une boîte cochée marquée " Disable (deny login) " : cliquez deux fois dessus pour la décocher entièrement



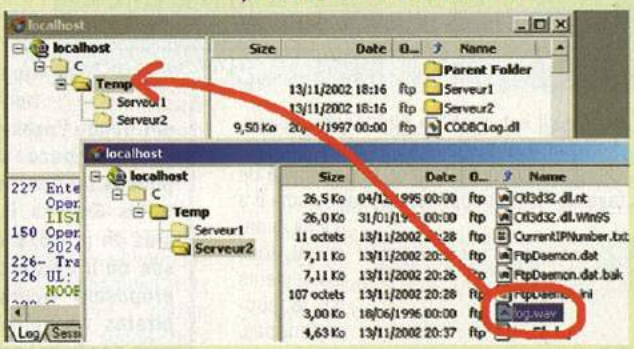
- toujours dans cette fenêtre, cliquez sur l'onglet " File Access ", puis sur le bouton " Add ", tapez le chemin " C:\Temp ", cliquez sur OK, puis deux fois sur " Read " et deux fois sur " Write " dans la partie " Files " à droite, et enfin une fois sur " Root " et " Home " dans la partie " Special ":
- cliquez sur OK, puis sur l'icône en forme d'éclair en haut à gauche pour lancer le serveur.



UTION DU WAREZ

Vous voilà prêt pour le FXP ! Lancez SmartFTP, et tapez l'adresse " localhost " et le port 21, cochez Anonymous, puis appuyez sur Entrée :

Une fenêtre doit apparaître, montrant l'arborescence de votre répertoire C:\Temp. Fantastique n'est-ce pas ? Maintenant, changez le 21 en 22 dans la case du port, et réappuyez sur Entrée pour vous connecter sur votre second serveur.



C'est bien sûr inutile, mais supposons que vous voulez copier le fichier " \Temp\Serveur1\log.wav " du serveur 2 dans le répertoire " \Temp\ " du serveur 1 : faites simplement un glisser / déposer entre les deux fenêtres :

Ca y est ! Vous avez fait du FXP, toutes mes félicitations ! Vous pouvez maitenant aller frimer devant vos copains, par contre ne leur dites pas que les serveurs étaient sur votre machine, tout de suite ça fait moins bien. Si vous êtes sous Linux, ça sera moins facile. Comme client, vous pouvez toujours utiliser PFTP [3], l'utilisation est un brin moins évidente que SmartFTP mais puisque vous avez installé Linux ce n'est pas de faire du FXP en mode texte qui devrait vous effrayer !

D'ailleurs, vous pouvez même utiliser le client de base que l'on trouve sur toutes les distribs, mais là l'intérêt est plus théorique que pratique... Comme serveur, un serveur quelconque devrait convenir, mais si vous voulez le top du top, essayez glftpd [5].

COMMENT ÇA, ÇA SERT À RIEN ??

Il faut bien reconnaître que pour copier un fichier d'un répertoire à un autre sur votre disque dur, le FXP n'est sans doute pas la méthode la plus simple. En fait, le principal intérêt du FXP réside dans cette simple constatation : si le transfert se fait de serveur à serveur, sans que les données transitent par votre machine, alors la vitesse de transfert ne dépend pas de votre connexion. Que vous ayez l'ADSL, un vieux modem 28.8 ou une ligne dédiée 100 Mbits/s, vous obtiendrez la même vitesse. Si par exemple vous n'avez qu'un simple modem, vous pouvez demander à votre pote qui lui a l'ADSL d'ouvrir un serveur FTP, et pour télécharger un gros fichier, vous ferez du FXP entre le serveur distant et son serveur à lui. Vous pourriez aussi utiliser la connexion de votre école ou université pour faire de même (attention, là, pensez à lire le règlement de l'établissement pour vérifier que c'est autorisé !).

Un autre intérêt du FXP, c'est de pouvoir cacher son adresse IP, si vous êtes soucieux de protéger votre identité. Généralement, un serveur FTP loggue les adresses IP des utilisateurs, mais il est possible de se connecter via un proxy pour ne pas montrer sa véritable IP (un proxy est un serveur qui relaie les données que vous envoyez vers le serveur FTP auquel vous vous connectez, ce qui donne au FTP l'impression de dialoguer avec le proxy). L'inconvénient d'une telle méthode, c'est que les données que vous recevez doivent aussi passer par le proxy, et la vitesse de téléchargement dépend donc de la vitesse du proxy (qui, s'il est public, est souvent assez limitée). MAIS, si au lieu de télécharger, vous faites du FXP vers le serveur FTP que vous avez installé sur votre machine, le serveur internet va envoyer les données vers votre serveur local, sans passer par le proxy (cela dépend aussi du type de proxy, les proxies dits de type " Socks " fonctionnent ainsi en tout cas). Résultat, l'IP apparaissant dans le log est celle du proxy, mais vous pouvez télécharger à la pleine vitesse de votre connexion ! Attention tout de même, vous n'êtes pas totalement invisible, puisque pendant le transfert l'administrateur de la machine hébergeant le serveur FTP peut très bien voir votre IP, une connexion active existant avec votre propre serveur.

FXP ET [IL]LÉGALITÉ

Le FXP en lui-même n'a absolument rien d'illégal, et pourtant il est aujourd'hui au coeur d'une grande part du piratage underground du net. Je vous rappelle (voir encore le n°4), qu'il existe de gros serveurs FTP, appelés des " Sites ", qui sont utilisés par les groupes pirates pour publier et distribuer leurs releases (les logiciels, films, ... piratés). Or, comment les fichiers passent-ils d'un serveur à l'autre ? Par FXP bien sûr !! Je prends un exemple : un membre d'un groupe de DivX, après avoir " rippé " un DVD pour le convertir au format DivX, doit uploader le film sur les 5 sites auxquels son groupe a accès. Il ne va uploader que vers UN seul site, et ensuite lui (ou ses collègues), se chargeront de le copier, grâce au FXP, vers les 4 autres sites. Et une fois que le film est mis à la disposition de tous sur ces 5 sites, il sera dupliqué, toujours par FXP, vers tous les autres sites sur le net ! Les sites étant très rapides (10, 100 Mbits, voir 1GBits), en quelques minutes un film entier se retrouve dispo sur une multitude de serveurs pirates.

Mais la chaîne de distribution est encore loin d'être finie à ce point. En effet, des petits malins ont remarqué qu'il existait beaucoup de serveurs FTP publics sur le net autorisant l'upload (généralement les ser-

PIRAT'Z

ELLE PIRATAIT WINDOWS : 9 ANS DE PRISON

Lisa Chen, 52 ans, risque de regretter lourdement son rôle dans le piratage et la revente de logiciels informatiques puisqu'elle a écopé de 9 ans de prison ferme et de 11 millions de dollars de dommages et intérêts. C'est la peine la plus lourde jamais infligée par un tribunal américain à un non-récidiviste. Arrêtée en novembre 2001 à Los Angeles, Lisa Chen faisait partie d'un réseau qui s'était enrichi de 98 millions de dollars en piratant des produits Microsoft, comme Windows XP et Microsoft Office 2000 Pro. Elle pourra méditer aux conséquences de son acte... jusqu'en 2011 !

EMBROUILLE AMAZONIENNE

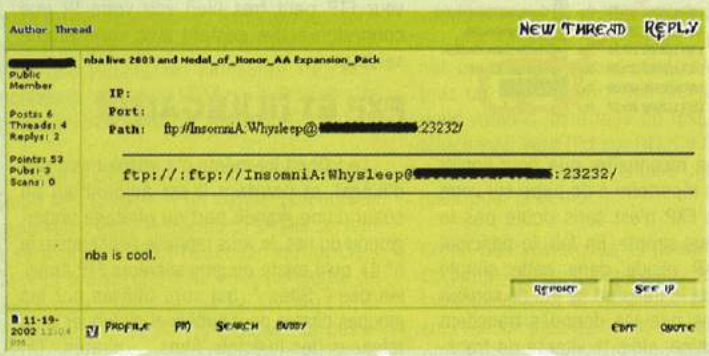
Lorsque l'internaute tape dvdpascher.com, il est redirigé vers Amazon. Le tout au détriment de dvdpascher.net, un vrai moteur de comparaison de prix de DVD, lui-même partenaire d'Amazon ! Ce bel embrouillaminis fait en tout cas une pub gratuite au géant Amazon. Quant au propriétaire de dvdpascher.com, ses motivations sont plus qu'obscures. On sait que le nom de domaine a été déposé par une société israélienne, Tropictel.com, éditrice de sites pornographiques...

veurs de compagnies, qui pouvaient ainsi recevoir des fichiers, ou qui étaient tout simplement mal configurés). Ils ont eu alors l'idée d'utiliser ces serveurs pour distribuer des logiciels piratés : il suffit d'uploader sur le serveur, puis de dévoiler l'adresse pour permettre à d'autres de télécharger. C'est ce qui a donné naissance aux boards FXP, et c'était en 1998 (cette information vient d'un administrateur d'un des plus vieux boards existant, avec lequel nous avons pu discuter sur IRC).

Un board FXP, c'est un forum hébergé sur un site web, sur lequel sont postés des liens vers des FTP au contenu souvent pas très légal. Cette image est tirée d'un board public (sur lequel n'importe qui peut s'inscrire), et montre un exemple de ce qu'on peut y trouver :

[UPDATE] Mp3: 25 AlbumZ [/UPDATE]	rvN69	0	9	11-15-2002 09:02 AM by rvN69	
[one game [/100 mbit]	Histerio	0	15	11-14-2002 03:08 PM by Histerio	
appz stro	bleemz	1	8	11-14-2002 02:51 PM by Histerio	
[Mp3] 10 Full Albums	rvN69	1	11	11-14-2002 12:47 PM by Histerio	
[Stro] 6 BookZ - AppZ - 4 GameZ - 1 DVDrip - 3 AlbumZ [/Stro]	rvN69	1	16	11-14-2002 12:46 PM by Histerio	
[UPLOAD] NBA Live 2003 [MYTH] + KeyGen	-= mAc =-	1	14	11-14-2002 12:45 PM by Histerio	

Dans chaque thread (un sujet de discussion dans un forum) est posté un lien vers un serveur pirate, comme ici:



Les membres du board n'ont alors qu'à copier ce lien dans leur client ftp, et le tour est joué, ils peuvent télécharger NBA Live 2003 ou l'add-on de Medal of Honor avant même leur sortie en France !

Pourquoi le nom de " Board FXP " ? Parce que, bien entendu, les données piratées uploadées sur le serveur peuvent être uploadées par FXP, et non pas obligatoirement à partir de la machine du pirate (qui dispose rarement d'une connexion très rapide). C'est pour cela qu'on peut voir apparaître sur des FTP publics des jeux qui ont été sortis moins d'une heure auparavant sur un Site par un groupe pirate.

LA CHASSE AUX FTP, UN SPORT TRÈS À LA MODE

Lorsque les boards FXP ont été lancés en 1998, ils s'appuyaient sur une constatation simple : il existait des milliers de serveurs que les entreprises ou universités laissaient en libre accès sans contrôler le moins du monde ce qui pouvait se passer dessus. Trouver un tel serveur n'est pas bien compliqué : il suffit de scanner sur le port 21 une partie du réseau internet (interroger tous les ordinateurs entre les adresses IP 192.168.0.0 et 192.168.255.255 par exemple (je vous déconseille cet exemple quand même, vous ne trouverez pas grand chose d'intéressant)). Pourquoi le port 21 ? Parce que c'est le port par défaut des serveurs FTP. Ensuite, si le programme de scan est assez évolué - comme l'un des plus utilisés sur les boards, Grim's Ping [6] - il va tester les FTP trouvés en vérifiant qu'il est possible d'uploader dessus, d'effacer éventuellement, et aussi de télécharger. Additionnellement, la possibilité de faire du FXP est aussi testée, car comme il a été dit auparavant, tous les serveurs ne le supportent pas. Une personne qui scanne ainsi les FTP est appelée un scanner (sur un board FXP). Il peut utiliser les serveurs qu'il a trouvés pour les remplir lui-même, mais il va souvent poster la liste sur le board pour permettre à d'autres de les remplir. C'est à cela qu'est dédiée la section " Scans " d'un board, et on y trouve des posts remplis de FTP scannés avec leurs caractéristiques (cela dépend bien sûr du logiciel utilisé) comme :

```
192.168.0.1
-------------
DIR: /upload/
DELETE STATS: nondeletable
RESUMABLE: Yes
SEND SPEED: 5123,40 bytes/s

192.168.0.23
-------------
DIR: /
DELETE STATS: deletable
RESUMABLE: Yes
SEND SPEED: 5119,00 bytes/s
.....
```

COMMENT LE FTP A DÉTRÔNÉ LE WEB

Avant l'apparition des boards FXP, la source privilégiée de warez sur le net était la multitude de sites proposant en téléchargement libre des logiciels qui l'étaient moins. Mais, comme on vous l'a expliqué dans le premier Pirat'gamez, les sites Web de warez sont peu à peu devenus d'immenses réservoirs à pop-ups sans contenu réel. Le problème du Web, c'est évidemment la bande passante : les pirates utilisent l'espace offert par des hébergeurs gratuits, qui se rendent souvent vite compte de la supercherie en constatant l'énorme débit causé par la présence de fichiers pirates. Du coup, ces fichiers ont une espérance de vie extrêmement limitée. Les créateurs de sites pirates ont donc cherché d'autres solutions, et ce sont les boards FXP qui leur ont donné l'exemple : il suffit d'utiliser l'espace de serveurs FTP publics au lieu des pages web gratuites. En plus, il y a généralement plus de place. C'est pour cette raison qu'il existe des sites web qui proposent toujours des logiciels pirates en téléchargement, mais avec des liens vers des serveurs FTP. L'utilisation de serveurs FTP, publics ou privés, a donc dépassé le cadre des boards FXP : outre les groupes accessibles via le Web, d'autres donnent sur IRC les liens vers les fichiers qu'ils ont uploadé.

Mais, le temps passant et les boards FXP devenant de plus en plus à la mode (il y en a aujourd'hui des centaines, voire des milliers), les administrateurs réseau ont fini par se rendre compte de l'usage illégal qui pouvait être fait de leur serveur. Par conséquent, le nombre de FTP publics est loin d'augmenter aussi vite que le nombre de FXPers (les membres des boards). Et il a été observé (depuis l'année 2001 en gros) un surpeuplement des serveurs FTP qui a conduit la scène des boards FXP à changer un peu de visage.

NOOS FAIT PEUR

Noos a décidé de lancer un vaste plan de lutte contre les fraudeurs qui accèdent gratuitement aux chaînes de l'offre Noos TV, via des cartes pirates. La société estime qu'en Ile-de-France, " plusieurs milliers d'immeubles " se délectent devant les 100 chaînes sans leur acquitter le moindre versement. Incapable de

FXP, TON UNIVERS IMPITOYABLE

A l'origine, un certains nombre de règles ont été édictées par les boards FXP de manière à " réglementer " l'accès aux pubs (un pub = un serveur FTP public). On peut souvent les trouver sur les boards, et on notera notamment que :

1) il est interdit d'effacer quoi que ce soit
2) il est interdit d'uploader sur un pub qui est en cours d'utilisation par un autre FXPer
3) il y a toujours au moins trois règles

La règle 1 a toujours été violée par des individus jugés malfaisants par les FXPers, appelés logiquement les " deleters " (= ceux qui effacent). Que fait un deleter ? Il s'amuse à aller effacer les fichiers uploadés par les membres du board, ce qui n'est souvent pas bien difficile puisque la plupart des pubs autorisent l'effacement de fichiers. Pour quelle raison fait-il ça ? On peut en imaginer plein, qu'il lutte contre le piratage, qu'il méprise pour une raison ou pour une autre les boards FXP et veut leur causer quelques soucis, qu'il est lui-même un FXPer sur un autre board qui veut récupérer l'espace disque du serveur pour ses prores uploads... Toujours est-il qu'il existe de telles personnes, qui sont un peu la hantise des boards FXP. C'est en grande partie pour éviter cela que de nombreux boards sont privés (on ne peut pas y rentrer sans y être introduit), et que quasiment tous ont une section privée à laquelle on n'accède que si on a suffisamment contribué. La contribution justement, c'est aussi un point clé du fonctionnement des boards FXP : il existe de très gros boards (plusieurs milliers de membres), et des beaucoup plus réduits (quelques dizaines). Mais, comme nous l'a expliqué l'administrateur d'un board, " ce n'est pas la quantité qui fait la différence, mais la qualité. Les boards les plus réputés de la scène FXP sont aussi les plus petits, sur lesquels tout le monde participe énormément, car sur un tel board ne pas participer signifie perdre son accès. Sur les gros boards, il est impossible d'avoir un tel contrôle, et il y a toujours plus de leechers, de stealers ou de deleters ".

Les deleters on connaît déjà, mais qu'est-ce qu'un leecher ou un stealer ? Un leecher, c'est quelqu'un qui profite des autres en téléchargeant beaucoup sans rien donner en échange (" a leech " en anglais, c'est une sangsue). Ceux-là ne sont bien sûr pas les bienvenus sur un board FXP, mais il y en a toujours sur les boards publics (apparemment, certains ouvrent un compte sur un board dans le seul but de télécharger un maximum avant de se faire virer, ce qui, bien entendu, met en rogne les admins des boards). " Stealer ", quant à lui, est un terme qui désigne deux catégories de personnes :

- ceux qui " volent " les FTP des autres pour y uploader à leur place (donc c'est aussi dans ce cas un deleter), ou pour les poster sur d'autres boards sous leur propre nom
- ceux qui " volent " l'adresse du FTP pour la diffuser ailleurs (pas seulement sur des boards)

Ces deux catégories ont tendance à grossir de plus en plus au fur et à mesure que le temps passe. En effet, le manque de FTP publics force les FXPers à chercher parfois pendant des heures parmi des scans un FTP sur lequel ils pourraient uploader dans les règles. Certains ne sont pas assez patients et effacent le contenu du premier qu'ils trouvent pour se l'approprier, ou font semblant de ne pas remarquer qu'il est déjà utilisé. D'autre part, il existe des endroits (channels IRC, sites web) où sont postés des liens "trouvés" ("volés", pour les FXPers) sur les boards FXP, et qui sont ainsi mis à la disposition de beaucoup plus de monde qu'il n'était prévu. On m'a montré par exemple un tel channel IRC, où sont postés uniquement des liens venant de boards FXP, qui contient en permanence plus de 600 personnes : en 30 minutes, 110 personnes ont tapé la commande qui envoie la liste des liens, ce qui à ce rythme fait plus de 5000 par jour !!

HISTOIRE DROLE DU FXP: UN DELETER, UN STEALER ET UN LAMER SONT DANS UN BATEAU. LE BATEAU COULE. QUI EST SAUVE ? LE BOARD FXP.

Pourquoi les FXPers détestent-ils tant ces channels (ou sites web) ? Déjà parce qu'un des principes fondamentaux d'un board FXP, c'est le fait qu'un membre doit remercier celui qui a uploadé ce qu'il est en train de télécharger. Or, en dehors du board, il n'y a évidemment plus de remerciements. Mais surtout, un FTP sur lequel se ruent des centaines de gens va forcément saturer, donc devenir inutilisable (car trop lent ou toujours plein), et va très probablement être détecté par l'administrateur du serveur, qui n'aura plus assez de bande passante pour visiter ses sites X et va donc devoir s'attaquer au problème.

LES HACKERS À LA RESCOUSSE

Face à la pénurie de pubs, la scène FXP a vécu en 2001 une période de doute pendant laquelle de nombreux " anciens " se sont demandé si elle n'allait pas s'autodétruire. Mais au même moment est apparue une alternative au serveurs publics (" pubs ") : les serveurs hackés (" stros ").

Avant de rentrer dans les détails de l'étymologie du mot " stro ", qui passionnera sans doute nos lecteurs avides de connaissances littéraires, de quoi s'agit-il ? En fait, tout simplement, de hacker une machine sur le net et d'installer dessus un serveur FTP.

Tout simplement ? A priori, prendre le contrôle d'un serveur d'une entreprise, ce n'est pourtant pas à la portée du premier venu ?! Et bien si, grâce à notre bon ami Microsoft qui a eu la bonne idée d'inclure une vulnérabilité énorme dans son serveur web IIS, versions 4 et 5 [7]. Bien que le patch la corrigeant soit disponible depuis octobre 2000, nombreux sont les serveurs qui n'ont pas été mis à jour, ou qui sont encore installés aujourd'hui sans la mise à jour. Cette faille a rapidement été exploitée par des hackers au service des boards FXP, qui se sont mis à scanner le net non plus à la recherche de pubs sur le port 21, mais de serveurs Microsoft vulnérables sur le port 80 (il existe des scanners spécialisés pour les trouver). Ensuite, la méthode pour les hacker est très simple et connue de nombreux FXPers :

'Z

localiser géographiquement les utilisateurs frauduleux. Nous prône la manière douce : prévenir et communiquer, via une campagne de dissuasion. Toutefois, l'opérateur, conscient de la difficulté de lutter contre les fraudeurs, ira jusque brandir le spectre de la prison pour les plus récalcitrants, afin des les effrayer un peu. Nous, on pense que pour endiguer efficacement le phénomène des cartes pirates, peut-être que réduire les tarifs... comment ça, non ?

TOUT SUR LE PEER-TO-PEER

Allez hop, un nouveau site à rajouter dans notre Best-of : http://www.ratiatum.com. En français et dédié à l'actualité du Peer-to-Peer, vous y trouverez toutes les dernières sorties en matière de logiciels, les ragots du piratage, des dossiers, des forums, des articles philosophiques, mais pas de bouchons en liège. Dommage.

L'EMPIRE D'HOLLYWOOD CONTRE-ATTAQUE

Cinq des plus importants studios de cinéma hollywoodien ont décidé de lutter activement contre le piratage de leurs catalogues sur Internet en lançant un site payant de films, Movielink. Lassés de voir les internautes piller leurs ressources cinématographiques, les cinq studios (Metro Golwyn Mayer, Paramount, Sony Pictures, Universal et Warner Brothers) ont investi à cet effet 100 millions de dollars. Les films seront à louer pour la journée, pour un coût allant de 3 à 5 dollars. 175 films sont dès aujourd'hui disponibles sur le site de Movielink (http://www.movielink.com). Ce service n'existe pour le moment qu'aux Etats-Unis. Toutefois, entre les "quelques" 175 films proposés par Movielink et l'offre pléthorique gratuite existant sur les réseaux peer-to-peer d'Internet, il est probable que les internautes feront vite leur choix...

LA MORT ANNONCÉE DES BOARDS FXP

Depuis la " pénurie " en serveurs publics, la mort des boards FXP a été souvent annoncée, et pourtant ils sont toujours extrêmement populaires. En fait, leur mort sera sans doute effective lorsque tous les administrateurs réseau du monde seront compétents, ce qui à mon avis n'arrivera pas avant un bon bout de temps : d'après mes estimations, autour de la même date à laquelle Microsoft sortira un produit non buggé. Bref, il y a de la marge. Et, si ce jour finit par arriver, avec l'évolution des technologies les particuliers auront sans doute accès à ce moment à des connexions bien plus rapides que l'ADSL : dès lors, plus besoin de chercher des serveurs à pirater, il n'y aura qu'à utiliser sa propre connexion ! Reste à voir où ira la préférence des utilisateurs : FTP ou P2P ? Réponse dans notre numéro 47 !

- uploader les fichiers d'un serveur FTP sur la machine distante en utilisant par exemple le programme TFTP qui est installé par défaut sur tous les Windows
- lancer le serveur FTP en mode " invisible ", en le configurant si possible pour qu'il redémarre après un reboot

Au début confidentielle, cette méthode est maintenant très répandue et a été étendue à d'autres types de failles, le principe étant toujours de prendre le contrôle d'une machine rapide pour y installer un serveur FTP. Car s'il y a maheureusement toujours des serveurs IIS vulnérables, leur nombre a quand même beaucoup diminué " grâce " à des virus célèbres comme Nimda, qui exploite cette faille (entre autres) pour infecter les serveurs web. D'une manière générale, la plupart des failles énormes et faciles à exploiter se retrouvent dans des virus, ce qui a au moins le mérite de les faire remarquer plus rapidement (plutôt que d'attendre qu'un pirate vienne installer dessus un énorme serveur warez).

Les avantages des serveurs hackés sur les serveurs publics sont :

- la vitesse : le hacker choisit de préférence une machine avec une bonne connexion internet
- pas d'accès anonyme (il faut un login / mot de passe) ce qui fait que personne ne peut trouver le serveur juste en scannant (il est aussi installé sur un port différent du port 21 pour cette raison). Voir la photo d'écran où l'adresse du FTP a été postée pour un exemple
- un meilleur contrôle : choix du nombre de comptes autorisés, visualisation de l'activité du serveur... Il y a souvent un message d'accueil sur les serveurs hackés, qui montre des stats qui peuvent être assez impressionnantes comme :

```
220-
220-
==========
220-
220-Ammout of Logins Since Server Started: 311 total
220-Logged in Users:    10
220-Total Kb downloaded:    41097520 Kb
220-Total Kb uploaded:      1842846 Kb
220-Ammout of Files downloaded:  2874
220-Ammout of Files uploaded:    128
220-Average Speed: 83.005 Kb/sec
220-Current Speed: 564.552 Kb/sec
220-Free Disk Space:  1891.92 MB
220-
220
==========
```

Et pour finir sur les " stros ", d'où vient donc ce nom bizarre ? J'ai trouvé plusieurs explications, la plus cohérente étant la suivante : à l'origine étaient les " distros ", qui sont des serveurs privés à partir desquels les groupes faisaient du FXP. Les serveurs hackés se sont alors vus appeler des " pubstros ", mélange de pubs et de distros. Et " stros ", c'est leur diminutif affectueux ;-)

```
220-
==========
220-  ©©© Welcome To ********* Server ©©©
220-
==========
220-
220-You are Connecting From ***.***.***.***
220-The Local time is 15:37:17,
220-1160 users have visited in the last 24 hours.
220-This server has been running since
220-5 Days, 23 Hours, 42 Mins, 14 Secs
```

QUELQUES LIENS UTILES :

[1] FLASH FXP, LE ROI DU FXP (SHAREWARE) :
http://www.flashfxp.com/download.php

[2] SMART FTP, LE MEILLEUR DES CLIENTS GRATUITS :
http://www.smartftp.com/download/

[3] PFTP, UN CLIENT POPULAIRE SOUS LINUX :
http://pftp.suxx.sk/pftp/

[4] WARFTP DAEMON 1.65, UN SERVEUR FTP FACILE À INSTALLER :
http://download.jgaa.com/ftp/pub/products/Windows/WarFtpDaemon/1.6_Series/ward165.exe

[5] GLFTPD, LE SERVEUR FTP SOUS LINUX :
http://www.glftpd.org/

[6] GRIM'S PING, UN SCANNER SIMPLE ET COMPLET SOUS WINDOWS : http://grimsping.cjb.net/

[7] BULLETIN DE SÉCURITÉ MICROSOFT, SUR LA FAILLE DANS IIS :
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

L'EMULATION POUR LES NULS

Que vous soyez un débutant complet en matière d'émulation, ou avide des dernières nouvelles, le site http://www.emu-france.com/ devrait satisfaire tous ceux qui ont quelques difficultés avec la langue de Shakespeare. On y trouve toute l'actualité de l'émulation, des articles qui permettront aux nouveaux venus de s'y retrouver, ainsi que tout plein de liens utiles, d'outils divers...

LISTEN.COM Y CROIT. PAS NOUS

Le site de téléchargement de musique payant Listen.com, où les catalogues d'Universal Music et de Warner Music sont disponibles, est le premier site à mettre en place un service -payant, of course- de gravure de CD. Pour lutter contre le piratage, plus de 75 000 chansons pourront être gravées sur un CD vierge, au prix de 0,99 dollars la chanson. Elles seront distribuées sous le format Windows Media Audio, mais seront converties dans un fichier son traditionnel pour permettre la gravure sur des CD qui pourront être joués sur n'importe quel lecteur. Toutes les initiatives sont bonnes pour contrer Kazaa et Morpheus, mais on sent bien que les majors américaines ne sont pas prêtes de remporter la partie qui les oppose aux millions d'internautes adeptes du peer-to-peer.

ACHETEZ DES XBOX POUR RUINER MICROSOFT !

Il est courant que les constructeurs de console vendent une console à perte : le prix très bas d'une console est un de ses arguments de vente les plus importants face à la concurrence des autres consoles et des ordinateurs. Les bénéfices se font ensuite sur les jeux achetés, c'est aussi pour cela qu'ils sont si chers. Microsoft a enfin révélé qu'ils perdaient pas moins de 120 $ par Xbox. Le total du déficit du département "Home and Entertainment" de MS est de 177 millions de $ sur les 3 derniers mois. "Tout va bien", assure Billou, "les pertes sur la Xbox sont facilement compensées grâce aux pigeons qui achètent toujours Windows pour leur PC". Conclusion : faites-moi plaisir, achetez tous une Xbox et installez Linux dessus.

LE JEU ÇA TUE

Un joueur Sud-Coréen de 24 ans est mort après une overdose de jeux vidéo. Il est resté pas moins de 86 heures à jouer sans dormir ni manger. La police n'a pas précisé où il en était en nombre de frags.

PEER-TO-PEER : LA BATAILLE CHANGE DE TERRAIN

Les sociétés luttant contre le piratage sur les réseaux Peer-to-Peer ont commencé par s'attaquer aux fournisseurs du service (Napster, AudioGalaxy, Kazaa,...). Bien que cette forme de lutte soit toujours d'actualité, elle a quand même montré ses limites : le temps de faire disparaître un réseau P2P, deux autres se sont déjà formés pour le remplacer. Du coup, l'idée de faire payer les utilisateurs (les vrais pirates, après tout) a fait son petit bonhomme de chemin. Bien sûr, il est inimaginable de faire un procès à tous ceux qui partagent un fichier illégal. Mais ce que veulent les compagnies, c'est faire des exemples, pour décourager au maximum les gens de prendre le risque. Le problème ? Il est à la fois technique et juridique : il faut repérer ceux qui partagent des fichiers copyrightés, puis obtenir leur adresse IP, et enfin demander au fournisseur d'accès les données personnelles de cette personne (le point le plus controversé). En espérant que la preuve de photos d'écrans avec les fichiers partagés sera acceptée au tribunal. Beaucoup d'obstacles donc, mais un premier pas a été franchi au Danemark : le groupe antipiratage APG a obtenu les IPs d'utilisateurs danois, a réussi à récupérer leur nom auprès des fournisseurs d'accès, et leur a demandé de payer une amende (basée sur ce qu'ils partageaient : environ 8 euros l'album MP3, 40 euros le jeu) avant le 1er décembre. S'ils ne paient pas, ils seront poursuivis par APG en justice.

En France, attention : même s'il n'y a pas encore de précédents, ce qu'a fait APG au Danemark, c'est exactement ce que souhaite faire RetSpan en France (www.retspan.info). Le problème juridique des accords avec les FAI pour obtenir les coordonnées des pirates n'est peut-être pas encore totalement réglé, mais il ne serait pas étonnant que RetSpan se fasse remarquer dans un futur proche... Après tout, ce sont des professionnels. Il n'y a qu'à regarder cette pop-up fantastique sur leur page de garde, qui nous informe du nombre de fichiers téléchargés illégalement depuis ce matin, pour voir qu'ils maîtrisent parfaitement le javascript : 65795804 exactement, au moment d'écrire cette news. Un coup d'oeil au source de la page vous permettra de savoir quelle heure il était.

XBOX : LES MODCHIPS BANNIS ONLINE

Microsoft vient de lancer son service de jeu en ligne pour la Xbox, le Xbox Live Vendu environ 50$, il a connu un très grand succès... et a lancé une vive polémique. En effet, les premiers possesseurs de modchips ont été les victimes d'une bonne farce de la part de Billou : le Xbox Live est en effet capable de détecter les modchips, et les Xbox moddées se retrouvent alors purement et simplement bannies... pour toujours ! Même en enlevant le modchip, il est trop tard : Microsoft a stocké votre numéro de série, l'a soigneusement rangé dans sa liste " tel est pris qui croyait prendre ", et vous n'avez plus qu'à aller acheter une nouvelle Xbox. Officiellement, Microsoft agit ainsi pour empêcher la triche en ligne. Accessoirement, c'est aussi un excellent moyen de lutte contre le piratage.

Une semaine après le lancement du Xbox Live, on apprend que ça y est, le système de ban a été cracké ! C'est en tout cas ce que prétendent certains sites qui vont un peu vite en affaire. En effet, le groupe Team Assembly a bien annoncé avoir pu jouer en ligne après avoir changé le numéro de série de la Xbox et l'adresse MAC (members.cox.net/opensource/). MAIS, il s'agissait d'une Xbox qui n'était pas bannie ! Ce qui a échappé à pas mal de monde on dirait. Donc, pour rétablir la vérité, personne n'a encore trouvé (à l'heure actuelle) comment permettre à une Xbox déjà bannie de se connecter. Bien sûr, les gens cherchent des solutions, et le meilleur moyen de savoir où ils en sont, c'est d'aller voir sur les forums d'Xbox-Scene (www.xbox-scene.com). En attendant, la sortie du Xbox Live en France n'est pas prévue avant le printemps 2003, donc vous avez le temps de voir venir... encore que si vous voulez être les premiers à vous faire bannir, vous pouvez toujours vous inscrire au bêta-test.

ULTRAHLE CONTRE-ATTAQUE

UltraHLE est un émulateur Nintendo 64 très connu pour deux particularités : non seulement c'est un des meilleurs, mais il n'a connu qu'une seule et unique version, ses auteurs ayant décidé de ne pas continuer le développement. Les seules améliorations qui ont suivi consistaient à modifier certains fichiers pour améliorer la compatibilité. Et bien, quelqu'un a enfin repris le code et depuis début Novembre les nouvelles versions d'UltraHLE Alpha se succèdent, sur http://alpha.emulation64.com/. Pour l'instant l'accent a plus été mis sur la facilité d'utilisation que sur l'amélioration de la compatibilité, mais ce n'est qu'un début, et on peut s'attendre à voir des progrès faits dans ce sens dans le futur. Et Nintendo devenir tout rouge par la même occasion.

CLONYXXL RESSUSCITE

ClonyXXL, un des détecteurs de protection contre la copie les plus populaires (permettant d'analyser une protection pour déterminer comment la contourner), avait été abandonné... Mais il est de retour et il n'est pas content (enfin, c'est surtout les éditeurs qui ne sont pas contents). A télécharger sur http://gowap.fr.st/

DE LA SUPÉRIORITÉ DE LA MULE SUR L'ÂNE

EDonkey est un des logiciels de P2P les plus populaires, notamment en Europe. Mais son interface n'est pas toujours très pratique, et les options de configuration sont souvent limitées. L'équipe responsable d'eDonkey ayant arrêté son développement pour se consacrer à leur nouveau projet de P2P (Overnet), il n'y a plus vraiment d'améliorations à attendre. Du coup, eDonkey est de plus en plus remplacé par eMule, un client compatible mais mieux fait, plus riche et plus pratique (http://www.emule-project.net/). De plus eMule permet l'utilisation de mods, qui sont des sortes de plugins ajoutant de nouvelles fonctionnalités et / ou corrigeant des bugs. Vous trouverez plus d'infos là-dessus sur http://www.open-files.com/, un site consacré à eDonkey et ses émules (eMule et Overnet).

MICROSOFT DÉMONTRE SON SAVOIR-FAIRE ANTI-PIRATES

Avec la sortie du Service Pack 1 de Windows XP, Microsoft a fièrement annoncé que les pirates n'allaient plus pouvoir profiter impunément de leurs mises à jour. En effet, ils ont astucieusement " blacklisté " les cd-keys des versions pirates les plus répandues (celle du group DevilsOwn plus précisément) pour empêcher leurs possesseurs de mettre à jour leur système. Ceux-ci ont aussitôt changé leur numéro de série en téléchargeant le keygen adapté.

PLUS DE MP3 AU BUREAU

Les connections rapides des entreprises ont dernièrement été montrées du doigt. Soi-disant, les employés ne les utiliseraient pas que pour surfer sur des sites de cul et chatter sur caramail : il paraît aussi qu'ils téléchargent des MP3. Du coup, notre ami Macrovision, spécialiste ès protections en tout genre, vient de s'associer avec Websense pour développer des outils qui détecteront les fichiers piratés sur votre ordinateur au bureau (et sans doute aussi les logiciels de P2P les plus répandus). Atteinte à votre liberté ? Peut-être, mais vu qu'une société US a dû payer 1 million de dollars de dommages et intérêts en avril dernier à la RIAA à cause de MP3 partagés par ses employés, rares sont ceux qui veulent continuer à prendre un tel risque.

WINDOWS 2000 SUR XBOX

C'est Billou qui a dû en avoir un choc, en apprenant qu'on avait réussi à faire tourner Windows sur la Xbox : " Quoi ? Et comment je vais le vendre moi, mon Windows XB ? ". Surtout que ceux qui y sont parvenus sont en fait passés par Linux : une fois que Linux tourne, il suffit d'utiliser un logiciel d'émulation de PC et d'y installer Windows 2000... En rajoutant à la console un clavier et une souris, on peut alors travailler sur Office, se connecter en réseau local, etc. Et pour les jeux ? Redémarrez votre Xbox, elle est faite pour ça après tout !

WARCRAFT JOUER ONLI

Jouer à Warcraft III sur le net, c'est le pied ! Mais, ne pouvoir le faire que sur Battle.Net, ça l'est déjà moins... Un serveur peut être down ou soudain lagguer à mort (jouez les Undeads dans ce cas), il y a régulièrement des Orcs au QI négatif qui ruinent les parties, sans compter cette fâcheuse manie qu'à votre mère de tout jeter, y compris le boîtier CD qui contenait votre cd-key... Pour toutes ces raisons et d'autres encore, dans le Pirat'gamez n°5 il était question des différentes méthodes alternatives pour jouer online sans Battle Net. Vu qu'il y a eu quelques patchs depuis (Warcraft III en est à sa version 1.04), il m'a aussi fallu patcher l'article.

IZ

Le Messie se retire

Début octobre, China Messiah a annoncé l'abandon du Messiah-X, un modchip dédié à la Xbox. La raison ? Officiellement, les difficultés à garder un chip compatible avec les changements que Microsoft inclue dans chaque nouvelle génération de sa console, ainsi que le trop grand nombre de modchips disponibles. Bien sûr, l'attitude agressive de Microsoft envers les fabricants de Modchips n'a rien à voir dans cette décision.

MAME & Cie

MAME, l'émulateur de jeux d'arcade le plus connu et le plus complet, n'est par contre pas très facile d'utilisation. Si vous débutez et que vous cherchez des sites en français, allez faire un tour sur http://www.mame-univers.net/ ou http://www.mame-france.net/. De plus, si vous voulez revivre les mêmes sensations que devant une borne d'arcade, le clavier n'est pas le meilleur périphérique de jeu. Essayez de faire un tour complet avec les flèches du clavier pour faire un coup spécial à Street Fighter, et vous comprendrez ce que je veux dire. Il existe dans le commerce des manettes d'arcade dont c'est justement le but, la plus connue étant le HotRod. Mais ces produits sont très chers (compter minimum 200 euros)... la solution peut alors être de fabriquer soi-même sa manette : le site http://www.arcade-controls.com/ vous donnera toutes les idées dont vous avez besoin, si vous êtes un peu bricoleur.
Malgré les quelques 3000 jeux émulés par MAME, il en reste qui ne fonctionnent pas, et il existe des émulateurs alternatifs moins connus qui peuvent alors rendre un grand service. Donc si vous en avez marre que votre borne d'ar-

****** Start of Patch ******

1] Se passer du CD

Si vous n'avez pas encore mis jour votre Warcraft, vous pouvez le faire par l'auto-update de Battle Net, ou en téléchargeant le patch sur [1] (pensez à restaurer votre fichier war3.exe original si vous aviez installé auparavant un crack no-cd).

Ensuite, il existe plusieurs cracks no-cd pour la version 1.04, on en trouve un par exemple qui marche sur le site de Megagames [2] : cliquez sur " Game Fixes " dans la catégorie PC, puis allez voir à la lettre W.

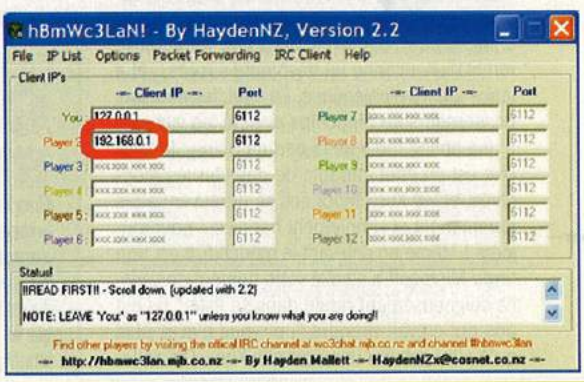
2] Jouer entre amis

Pour cela, il vous faut d'abord des amis. Ce n'est pas forcément le plus facile à trouver, mais pour ça je ne peux pas vous aider. Donc supposons que vous en ayiez (sinon, tout n'est pas perdu, continuez quand même à lire !). Ce qu'on va faire, c'est faire croire à Warcraft que vous êtes en réseau local avec vos potes. Pour cela, dans Pirat'gamez n°5, je vous disais d'utiliser le logicel Lancraft. Malheureusement, il ne marche apparemment plus avec la version 1.04. Heureusement, il en existe d'autres, et celui que nous allons utiliser est joliment nommé hBmWc3LaN! (ou encore Bidule dans la suite, pour éviter que vous vous étouffiez à la lecture de cet article). Vous pouvez télécharger la version 2.2, compatible avec Warcraft III 1.04, sur [3].

L'utilisation de Bidule est différente de celle de Lancraft : c'est le serveur qui doit lancer le logiciel et entrer les IPs des joueurs, alors que dans Lancraft c'étaient les joueurs qui devaient le lancer et entrer l'IP du serveur. Mais on va voir ça tout de suite...

Dans l'exemple qui suit je suppose qu'il y a deux joueurs. Celui qui va faire serveur lance Bidule et choisit le nombre de joueurs :

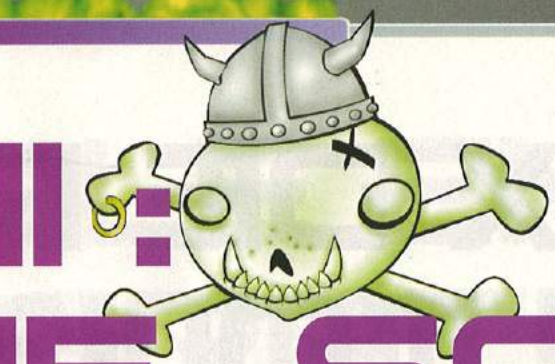
Ensuite, il entre les IPs des autres joueurs (rappel : taper ipconfig dans une boîte DOS pour avoir son IP). Il doit laisser l'IP marquée " You " sur 127.0.0.1 (on peut la changer si le serveur n'est pas sur la machine qui lance Bidule, mais c'est une utilisation particulière dont vous ne devriez pas avoir besoin) :



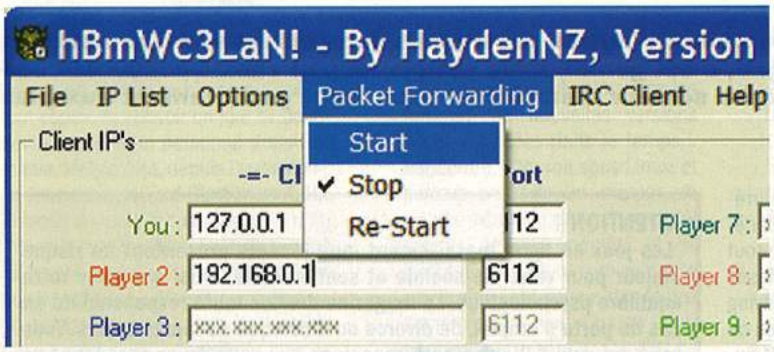
Il ne reste plus qu'à activer la redirection des paquets en faisant Start :

Et enfin, lancer le serveur (en choisissant bien " réseau local ").

Les joueurs, eux, cliquent sur " réseau local " pour voir la liste des parties, et doivent voir apparaître la partie en question. Il se peut qu'elle apparaisse plusieurs fois, ce n'est pas grave, choisissez celle que vous voulez !



III : NE SANS CD



Voilà, c'est tout ce dont vous avez besoin pour démarrer ! Bon jeu, et fouillez un peu dans les options de Bidule pour quelques fonctionnalités avancées. Ah oui, et si vous n'avez pas d'amis mais avez lu cette partie jusqu'au bout, il y a un channel IRC dédié à Bidule (le nom du serveur et du channel sont affichés par le programme, je ne m'aventurerai pas à les recopier). Apparemment, il n'y a pas grand monde là-bas, mais qui sait, je ne suis sans doute pas passé à l'heure de pointe. Ou alors, personne n'a réussi à taper l'adresse sans faute de frappe.

3] JOUER SUR BATTLE NET [OU PAS]

Officiellement, vous le savez sans doute, il est impossible de jouer sur Battle Net sans cd-key valide (les keygens dispos sur le net ne génèrent notamment pas de cd-keys valides). Les soi-disant cracks que l'on peut trouver sont soit des virus, soit une version de Kali (un programme qui permet de faire la même chose qu'en 2). Alors, c'est foutu ? Oui. Pourtant, un groupe pirate (KiNDRED) a sorti un crack intitulé " Warcraft III Original Registration CD Key File ", qui permet d'après eux de jouer sur Battle Net avec n'importe quel numéro de série. Je n'en avais pas parlé dans le numéro précédent car je n'avais pu trouver personne ayant testé ce crack (très peu répandu, il faut dire qu'il s'agit d'un fichier war3.mpq d'environ 400 Mo). Mais aujourd'hui je peux vous dire que... IL MARCHE !!! Calme, calme on reste calme !! Mais, car il y a un mais, il ne marche pas très bien. D'après la personne qui l'a testé pour nous, parfois le message " cette cd-key est en cours d'utilisation " apparaît. Pourquoi ? Difficile de le dire, il faudrait demander aux gars de KiNDRED comment il fonctionne. Mais l'explication qui me semble la plus logique est la suivante : ils ont simplement récupéré le fichier war3.mpq d'une copie de Warcraft III installée avec une cd-key valide (la cd-key est stockée, encryptée, dans ce fichier), et ont balancé ce fichier sur le net. Vu qu'il n'a été que très peu diffusé, peu de monde utilise cette cd-key et elle marche *de temps en temps*. Donc rien d'extraordinaire là-dedans...

De toute manière, ce qui nous intéresse ici ce n'est pas de jouer sur le vrai Battle Net, mais sur des serveurs officieux qui émulent les serveurs de Blizzard. Je ne vais pas vous rebalancer tout l'article du numéro précédent, nos fidèles lecteurs crieraient au vol, mais vu que certains sites ont changé, je vous fais un petit résumé :

- bnetd.org, parmi les premiers à offrir un support Battle Net de qualité, ne donne toujours pas signe de vie (l'action en justice de Blizzard à leur encontre doit donc continuer)
- le meilleur choix à l'heure actuelle, ce sont les serveurs PvPGN [4]
- tous les fichiers nécessaires pour jouer, ainsi que pour installer un serveur, sont disponibles sur [5]
- la liste de serveurs est accessibles via le site de PvPGN [4]
- si les infos ci-dessus ne sont plus à jour au moment où vous lisez cet article, remontez dans le temps
- ou, autre solution, allez sur le channel IRC de PvPGN : #PVPGN sur irc.pvpgn.org (lisez le topic)

**** End of Patch ****

[1] Le patch 1.04a français :
ftp://ftp.blizzard.com/pub/war3/patches/PC/War3Patches_104a_Francais.exe
[2] Megagames, la bible des cracks :
http://www.megagames.com/
[3] WCGalaxy, des tas de downloads pour Warcraft III (regardez dans la section Utilities, et pensez qu'il y a plusieurs pages) :
http://www.wcgalaxy.com/modules.php?name=Downloads
[4] PvPGN, un serveur Battle Net :
http://www.pvpgn.org/
[5] Tous les downloads pour PvPGN :
http://pvpgn.wwsecurity.net/

cade encombre votre salon, et que vous n'arrivez pas à la faire rentrer dans votre PC grâce à MAME, rendez-vous sur le site unMAMed pour savoir pourquoi, et peut-être trouver la solution : http://unmamed.mame.net/

Patricia Kaas n'est plus classée X

La chanteuse la plus connue de Moselle avait porté plainte le 28 août dernier contre la société Star en Direct, propriétaire d'un site pornographique au nom de la chanteuse. C'est l'OMPI (Organisation mondiale de la propriété intellectuelle) qui a tranché, donnant gain de cause à la star, représentée par la société " Tour de charme ", qui possède la marque Patricia Kaas. L'OMPI a mis en avant le fait que la société Star Direct avait enregistré et utilisé le nom de la chanteuse de " mauvaise foi " et a donc conclu qu'elle " n'avait aucun droit sur le nom ". Grâce à cette décision, Mademoiselle Kaas n'a plus le blues...

LES JEUX DE R BIENTOT TOUS

Se balader avec des centaines d'autres passionnés dans les mondes fantastiques des jeux de rôle en ligne, c'est génial, mais parfois un peu cher. Découvrez comment utiliser votre propre serveur d'émulation pour jouer gratuitement aux plus célèbres MMORPG !

FAITES VENDEUR DE MODCHIPS ON EMBAUCHE !

Le magasin en ligne Lik Sang (www.lik-sang.com), basé à Hong-Kong, était l'un des plus prisés par les amateurs de modchips : grande variété de choix, réputation de fiabilité... Bref, ils vivaient heureux et insouciants... Jusqu'à ce que le Prince du Mal, Microsoft, aidé de ses deux accolytes Sony et Nintendo, lance une attaque surprise (enfin, surprise... y z'auraient pu s'en douter quand même). Résultat, un procès bien fourni sur les bras, et un site web fermé pendant environ un mois. Incapable de gérer à la fois le procès et leur commerce, Lik Sang a finalement décidé de se faire racheter (par Pacifig Game Technology) : leurs acheteurs s'occupent du site web qui est de nouveau en ligne (sans les modchips et autres accessoires douteux bien sûr), tandis qu'eux tentent de gagner le procès. On leur souhaite bien du courage.

LINUX AIME LA XBOX

Linux sur Xbox, ça y est ! Le Xbox Linux Project (http://xbox-linux.sourceforge.net) a été couronné de succès, et vous pourrez télécharger sur leur site une distribution spéciale Xbox de la Mandrake 9, conçue pour s'installer le plus facilement du monde. Attention tout de même, il vous faudra un modchip pour pouvoir installer Linux. Les irréductibles attachés à Debian iront eux voir sur la page spéciale Debian : http://xbox-debian.linux.pt/. Quant à MacOS X, on n'a pas encore de nouvelles pour l'instant. Et je ne crois pas que Microsoft apprécierait de voir sa console transformée en Mac !

Pour les anglophobes irrécupérables et ceux qui débarquent, je rappelle tout d'abord que MMORPG signifie " Massively Multiplayer Online Role Playing Game ", ou encore en français " Jeu de Rôle en Ligne Massivement Multijoueurs " (JRLMM donc, mais personne ne le dit, vous pouvez toujours essayer de lancer la mode). Il s'agit de jeux comme Ultima Online ou Everquest, où le joueur incarne un personnage dans un monde imaginaire rempli de monstres, de trésors, de milliers d'autres joueurs et de lapins (espèce très dangereuse pour le joueur débutant d'UO).

La plupart de ces jeux sont malheureusement payants, et autour de 10 euros par mois, ils reviennent vite cher. Il existe certes des exceptions : notamment La Quatrième Prophétie [2] qui a en plus l'avantage d'être français, mais n'est pas aussi fouillé que ses concurrents venus de l'autre côté de l'Atlantique. Dans le Pirat'gamez n°5, nous vous avions expliqué comment jouer à UO gratuitement sur des serveurs non officiels, ainsi que comment créer votre propre monde virtuel.Le principe consiste à utiliser des serveurs gratuits (appelés " émulateurs " car ils émulent en quelque sorte le serveur d'origine), qui existent pour UO mais aussi pour d'autres jeux en ligne. Aujourd'hui, je vais donc vous donner un panorama plus général de l'émulation des MMORPG, afin de vous permettre d'y trouver votre bonheur. Avec les adresses des logiciels que je vous donne à la fin de l'article, vous pourrez télécharger et installer votre propre serveur d'émulation pour y inviter vos amis ou collègues dans de folles parties. Si vous êtes flemmard, vous pourrez aussi vous connecter sur les nombreux serveurs d'émulation publics existants sur Internet.

ATTENTION !

Les jeux en ligne massivement multijoueurs présentent un risque majeur pour votre vie sociale et sentimentale, ainsi que pour votre équilibre psychologique. Le magazine décline toute responsabilité en cas de perte d'emploi, de divorce ou d'attaque de lapins tueurs. Vous voilà prévenu ! D'autre part, rappelons que vous devez posséder une copie originale du jeu même si vous ne jouez pas sur un serveur officiel. Enfin, vérifiez dans votre licence que vous êtes effectivement autorisé à jouer sur le serveur de votre choix.

ULTIMA ONLINE

– LE DOYEN EST EN PLEINE FORME

Malgré ses 5 ans d'âge, le précurseur et archi-connu UO fait toujours recette auprès d'Origin, mais aussi dans la communauté de l'émulation MMORPG puisqu'il s'agit toujours du jeu qui fait l'objet du plus grand nombre de projets conséquents. Actuellement, ces projets sont suffisamment développés pour vous permettre de jouer dans des conditions comparables aux serveurs officiels d'Origin (avec moins de monde quand même bien entendu) : il existe des centaines de Shards (= des serveurs) gratuits sur lesquels vous pouvez jouer, chacun avec son propre monde, ses propres règles, ses propres guildes... bref, un univers immense à explorer pour qui osera s'y aventurer.

1) LE JEU

UO est vieux, et ça se ressent malheureusement sur le plan technique.

OLE EN LIGNE GRATUITS ?

Son monde est à la base un monde 2D, et passer à un monde en vraie 3D nécessiterait de tout revoir, ce qui enlève tout espoir de pouvoir un jour se balader à la première personne dans Britannia. Malgré tout, depuis l'extension " La Revanche de Lord Blackthorn ", UO dispose de modèles en 3D qui ont au moins le mérite d'améliorer la qualité du graphisme (qui reste cependant bien en deçà de ses derniers concurrents), et d'offrir un mode zoom (à l'intérêt quand même assez limité). De plus, la prochaine extension d'UO, " Age of Shadows ", doit sortir début 2003. Apparemment des efforts ont été faits du côté des graphismes, même s'ils restent encore en deçà des concurrents.

Alors, pourquoi UO est-il toujours au top ? Sans doute car il offre aux joueurs des expériences extrêmement diversifiées : il ne met pas l'accent uniquement sur les combats (comme Everquest), et donne la possibilité de faire évoluer son personnage dans des domaines extrêmement différents. Devenir un forgeron réputé, un dresseur d'animaux hors pair, faire fortune dans le commerce... autant de challenges qui raviront les joueurs chevronnés lassés du hack'n slash à la diablo. C'est donc aux joueurs plutôt expérimentés que je recommande UO, les nouveaux venus dans le monde des jeux de rôle préféreront sans doute un jeu plus beau, et dans lequel on débute plus facilement.

2) Les émulateurs

Côté émulateurs, le moins qu'on puisse dire c'est qu'il y a l'embarras du choix !

- Sphere [10] : c'est le serveur le plus utilisé par les Shards actuels. Son principal atout : sa simplicité d'installation et d'utilisation qui permet d'avoir facilement un monde complet prêt à accueillir des joueurs. Sphere approche maintenant de sa version 1.0 qui devrait logiquement s'imposer sur de nombreux Shards.
- Penultima OnLine (POL) [7] : un autre émulateur assez répandu, parmi les plus anciens. Il se distingue par sa relative complexité de mise en oeuvre (par rapport à Sphere), son site web assez peu mis à jour (il vaut mieux lire les forums), de nouvelles versions assez espacées dans le temps... Par contre, il tourne sous Linux, et surtout possède un moteur de scripts extrêmement puissant qui permet de tout modifier et de rajouter tout ce qui nous passe par la tête (oui, même des lapins sanguinaires). Les Shards tournant sous POL sont en général de très bonne facture.
- UOXClassic [13] : un autre parmi les " vieux " émulateurs, mais aujourd'hui un peu dépassé. Certains Shards assez anciens tournent encore avec cependant.
- UOX3 [12] : encore un émulateur qui a eu son heure de gloire, mais qui peine à tenir le rythme des meilleurs. Son avenir est de plus compromis par de sombres histoires de conflits entre le chef actuel du projet et d'autres personnalités de la " scène " de l'émulation.
- LoneWolf [5] : un émulateur assez discret mais dont le développement (basé sur de multiples versions d'autres émulateurs) est vraiment actif, avec des mises à jour (beta) très fréquentes. Il mérite qu'on garde un oeil sur lui (il tourne aussi sous Linux).
- Wolfpack [WOLFP] : assez proche de LoneWolf (en fait, LoneWolf est basé sur une ancienne version de Wolfpack). Il n'est pas non plus très répandu mais n'en n'est pas moins opérationnel.
- Nox Wizard [6] : un autre émulateur assez récent qui fait son petit bonhomme de chemin. Pas encore au top, mais déjà assez stable, donc utilisable.
- Epsilon [3] : un émulateur qui semble prometteur, mais qui en pleine réécriture à l'heure actuelle : il vaut mieux attendre de voir quels seront les progrès faits dans la prochaine version.
- RunUO [9] : sans doute l'émulateur le plus prometteur à l'heure actuelle. Il n'a été lancé que cette année, mais bénéficie de l'expérience de ses développeurs qui ont déjà travaillé sur d'autres émulateurs d'UO. Il n'est cependant pas encore suffisamment complet pour y faire tourner un Shard, donc il faudra encore patienter un peu. Les allergiques à Microsoft s'irriteront aussi de le voir programmé en C# (même leur site web est une véritable vitrine de pub pour Billou, à croire qu'ils sont sponsorisés !).
- Revelation [8] : un projet récent d'émulateur qui semble avoir pris du plomb dans l'aile (pas de mise à jour depuis bien longtemps). Et vu qu'il n'en est qu'à sa version 0.03a, il ne faut pas s'attendre à des miracles !
- Tupi [11] et Legend Server [4] : deux émulateurs récents en plein développement, et qui ont encore tout à prouver.

3) Les Shards

Là encore, il y en a pour tous les goûts, surtout pour les joueurs chevronnés amateurs de roleplay. En effet, l'un des objectifs des Shards, outre de vous permettre de jouer gratuitement, c'est aussi d'offrir une expérience de jeu différente de ce qu'on peut trouver sur les serveurs d'Origin. Chez Origin, n'importe qui peut jouer, du moment qu'il paie... il est même maintenant possible de payer plus pour pouvoir démarrer avec un personnage plus puissant !! Du coup, de nombreux joueurs se sentent désavantagés, ou se plaignent de newbies se comportant comme sur Diablo. Ceux-là devraient aller voir du côté des Shards privés, certains sont spécialisés dans le roleplaying, et demandent souvent aux nouveaux joueurs de détailler le background de leur perso avant de l'accepter. Mais il n'y a pas que des Shards de fanas de roleplay, il en existe aussi qui priviliégient l'action rapide, ou le PvP.

Maintenant, où les trouver, ces fameux Shards ? Si la barrière de la langue ne vous effraie pas, vous pouvez utiliser UO Gateway (voir la section " outils ") ou aller jeter un oeil sur le top 200 des Shards UO [17], vous trouverez certainement le Shard de vos

Et un piratage de plus pour la Nasa et le Pentagone !

Gary McKinnon, un pirate anglais de 36 ans de la banlieue de Londres, est inculpé aux Etats-Unis pour avoir pénétré dans 98 ordinateurs du Pentagone et de la Nasa, occasionnant quelque 900 000 dollars de préjudices. Les Etats-Unis exigent son extradition. L'avocat de McKinnon dénonce " la motivation politique " d'une telle extradition, car elle refuse de voir son client devenir un " exemple " pour la justice américaine. Et de rappeler que le pirate n'a aucun lien avec le terrorisme, supposition avancée un moment par les parties plaignantes. McKinnon avait en effet entre mars 2001 et mars 2002 copié des fichiers de mots de passe du Pentagone et effacé des comptes d'accès et des fichiers systèmes. Pendant trois jours, il avait privé de leur accès Internet plus de 2000 utilisateurs de la région de Washington ! Il risque 10 ans de prison et jusqu'à 1,75 millions de dollars d'amende. Mauvais temps pour les pirates du Web...

Microsoft sort ses chiffres du piratage

En octobre, Microsoft a annoncé avoir compté pas moins de 2 millions de sites web offrant la possibilité de télécharger des logiciels piratés, ou de commander de tels logiciels en ligne. Et alors ? Alors, ça fait beaucoup. Deux fois plus que l'an dernier d'après Microsoft. Et sûrement moins que l'an prochain d'après moi. Mais ça, Microsoft ne nous le dira que dans l'étude suivante.

rêves. Si vous préférez un Shard en français, le choix est moins vaste mais les plus connus sont sur la liste du site de Jeux Online [16].

4) Les outils

Il existe des tas d'outils dédiés à l'émulation d'UO. Certains sont à l'intention des créateurs des mondes, je vous renvoie à [1] pour les trouver. Je vais juste parler ici de ceux utiles au joueur :

- UO Rice [18] : certains Shards nécessitent que vous éliminiez l'encryption des données entre vous et le serveur, et c'est justement ce que fait cet utilitaire bien pratique
- Inside UO [22] : pas forcément utile, mais intéressant pour qui veut découvrir le monde d'UO sans le parcourir de fond en comble. Inside UO vous permet d'ouvrir les fichiers de données pour visualiser les persos, les sons, les cartes...
- Des fichiers de clients [CLIENT-SUO] : certains serveurs peuvent ne pas être compatibles avec votre version d'UO, vous aurez alors besoin de télécharger un autre client. Ce site vous donne des liens pour trouver ces clients.
- UOP [20] : il s'agit d'un CLIENT pour UO, sensé remplacer le client d'Origin. Le projet se veut même plus ambitieux maintenant, en voulant TOUT remplacer (le serveur, les outils d'édition...). Trop ambitieux peut-être, le projet semblant tourner un peu au ralenti en ce moment. Vous pouvez toujours aller jeter un coup d'oeil si vous ne possédez pas UO.
- UO Auto-Map [21]: un utilitaire qui vous permet d'afficher une carte détaillée, avec tout plein d'infos très utiles pour mieux comprendre le monde d'UO

EVERQUEST

– Sur les traces d'UO

Everquest (EQ), né de l'association entre Verant et Sony, est le second gros succès des MMORPG. Il est donc logique de voir que la communauté de joueurs s'intéresse à l'émulation de serveurs. Malheureusement, on est encore loin de ce qu'on peut voir sur UO, donc n'espérez pas pouvoir revivre la même expérience que sur les serveurs officiels.

1) Le jeu

Everquest a l'avantage par rapport à UO d'être entièrement en 3D. Il permet aussi au joueur de choisir parmi une quinzaine de races différentes, alors que les personnages joueurs d'UO sont désespérément humains. Les mécanismes de jeu sont aussi différents. EQ est résolument orienté exploration et combats : les joueurs partent à l'aventure (en groupe si possible, pour rester en vie plus longtemps) pour tuer des monstres, et ainsi ramasser de l'expérience, de l'argent et des objets magiques. Un concept simple mais qui plait, puisqu'EQ est le MMORPG le plus joué à l'heure actuelle.

2) Les émulateurs

Comme je l'ai déjà dit, les émulateurs actuels ne sont pas encore au niveau des " vrais " serveurs. En fait, ils sont conçus plus pour permettre aux joueurs de jouer sur un réseau local, plutôt que sur Internet. Ceci est en partie dû à la complexité du jeu (plus de données à envoyer de la part du serveur), et aussi à l'attitude agressive de Sony envers tout ce qui menace de près ou de loin ses produits : si les émulateurs EQ devenaient trop populaires, Sony risquerait de leur envoyer vite fait sa batterie d'avocats. Il existe tout de même deux émulateurs en développement :

- EQEmu [23] est le plus complet (ou tout du moins, jouable) à l'heure actuelle. Il est régulièrement mis à jour, donc surveillez les nouvelles versions pour voir où il en est.
- EthernalQuest [24] est moins avancé et progresse plus lentement (mais il progresse, c'est déjà ça). On regrettera quand même de ne pas pouvoir encore se battre, ce qui est un peu dommage dans un tel jeu ;)

3) Les Shards

C'est le plus gros point faible d'Everquest : on est très très loin des centaines de Shards d'UO. En fait, le seul Shard que j'ai pu trouver est le serveur de développement d'EQEmu, et vu qu'il n'existe aucune règle dessus, difficile d'espérer avoir une quelconque expérience de Jeu de Rôle. Pour l'instant, la seule manière d'utiliser un émulateur pour EQ est d'en installer un soi-même, si possible en réseau local pour ne pas avoir trop de lag. Mais on ne sait jamais, les émulateurs s'améliorant, peut-être verrons-nous bientôt des Shards en construction...

4) Les outils

Il existe actuellement très peu d'outils d'édition du monde d'EQ. Il y a bien sur le même site qu'EthernalQuest [24] quelques outils comme EQInside qui permet de visualiser le contenu des fichiers d'EQ, mais c'est à peu près tout.

Le joueur lui peut être intéressé par EQWindows [25] : il s'agit d'un programme qui permet de faire tourner EQ en mode fenêtré. Un outil très controversé est ShowEQ [26] : ce logiciel analyse les paquets venant du serveur et donne au joueur des informations qu'il n'est pas sensé avoir: il permet notamment de tricher, en voyant par exemple venir les lapins tueurs à l'avance. Ce programme est assez confidentiel, car difficile d'utilisation : il ne compile en effet que sous Linux, et il est donc nécessaire d'avoir une seconde machine pour l'utiliser (ou d'utiliser un émulateur comme VMWare). A n'utiliser d'ailleurs qu'à vos risques et périls, car ce faisant vous violez l'accord que vous avez passé avec Sony/Verant, et vous risquez d'être banni d'EQ (bien fait !).

ASHERON'S CALL

– Microsoft à la traîne

Asheron's Call (AC) est le MMORPG de Billou, qui décidément ne perd pas une occasion de mettre son nez là où il y a de l'argent à se faire. Graphiquement, il ressemble beaucoup à EQ (avec son monde en 3D), et malheureusement c'est aussi vrai du côté des émulateurs : s'il en existe, il n'est pas encore possible de trouver des mondes gratuits du niveau de ceux d'UO.

Le développement sur Xbox enfin légal

La Xbox, avec son architecture proche du PC, constitue un terrain d'expérimentation sans pareille pour tous les bidouilleurs en herbe. Jusqu'à présent, les développeurs étaient freinés par un problème de taille : pour compiler des exécutables, ils n'avaient à leur disposition que le SDK distribué illégalement sur le net. Mais une alternative est en train d'apparaître. L'émulateur Xbox commencé sur caustik.com/xbox/cxbx.htm (ne vous précipitez pas, il est loin d'être fini) a en effet permis de booster le développement d'OpenXDK, un kit de développement en open source dispo sur openxdk.sourceforge.net.

La France sera-t-elle le cancre de l'Europe ?

En cette fin d'année, il est temps de reparler de l'EUCD (European Union Copyright Directive), la directive européenne censée proposer une législation commune à l'Europe sur les problèmes de copyright et droit d'auteur. Cette directive est très contestée (voir www.eucd.org/issues/eucd/), notamment car elle est la source de restrictions sur le sacro-saint droit à la copie (c'est un peu l'équivalent du DMCA américain, voir ailleurs dans ces news). Mais une directive européenne n'est pas une loi : tous les pays membres doivent inclure dans leur système législatif les éléments de la directive, avant une date limite. Or, la date limite en question tombe le... 22 décembre 2002 ! Et, à notre connaissance, la France n'a encore rien fait dans ce sens (le projet de loi sur la Société de l'Information, qui aurait pu intégrer ces éléments, a finalement été abandonné). Monsieur le Premier Ministre, vous qui nous lisez, il vous reste à peu près une semaine. Au boulot !
Texte de la directive : www.fedepresse.org/la_presse_en_france/textes_fondateurs/textes/texte098a.htm

1) Le jeu

AC est donc très proche d'EQ : on reste dans le médiéval-fantastique tout ce qu'il y a de plus classique. AC se distingue notamment par des possibilités de développement des personnages plus variées, un système de magie assez spécial (chaque sort a une " formule " secrète, et sa puissance est d'autant plus grande que peu de gens la connaissent), et une hiérarchie sociale entre les personnages plus poussée. En tout cas, AC a bien marché, et d'ailleurs sa suite, astucieusement nommée Asheron's Call 2, vient de sortir. Mais nous ne sommes pas prêts de voir des émulateurs pour le 2, alors voyons ce que nous avonos pour le 1...

2) Les émulateurs

Les émulateurs pour AC ne se portent pas beaucoup mieux que pour EQ. Vous trouverez toutes les informations que vous cherchez sur ACdome [27], où vous apprendrez notamment qu'il y a déjà eu un certain nombre d'émulateurs commencés, mais que la plupart ont malheureusement stoppé le développement.

Tout n'est pas perdu cependant, puisqu'il en existe un qui continue bel et bien : UAS (Unified AC Server) [28], qui est encore très limité (il n'y a pas encore de monstres par exemple), mais compte bien devenir la référence de l'émulation sur AC (remarquez, c'est pas trop dur, vu la concurrence). UAS est en ce moment en train d'être complètement réécrit, et manifestement il va falloir attendre encore un peu avant de voir la nouvelle version. Mais on espère qu'elle nous apportera plein de bonnes surprises !

De plus, il y a en ce moment des rumeurs à propos de nouveaux émulateurs pour AC qui démarreraient, donc ill pourrait bien y avoir du nouveau dans un futur proche.

3) Les Shards

Comme sur EQ, les émulateurs ne sont pas encore suffisamment mûrs pour mettre en place un Shard digne de ce nom. Il faudra donc vous contenter des serveurs de test d'UAS, ou de celui d'ACdome. Ou d'installer vous-mêmes votre propre serveur.

4) Les outils

De spécifique aux émulateurs, il n'y a évidemment pas grand chose à se mettre sous la dent. Le site d'ACdome vous propose tout ce dont vous pourriez avoir besoin, notammment :

- les différentes versions des clients (comme pour UO selon le serveur, un client peut ne pas fonctionner)
- un programme pour gérer ses différents clients
- un programme pour visualiser les modèles d'AC, et un autre pour extraire les données (sons, textures, ...)

Si cela ne vous suffit pas, faites un tour sur [29], ce site recense une multitude d'utilitaires pour AC, bien trop pour tous les lister ici.

Dark Age of Camelot

– Le MMORPG nouvelle génération

Dark Age Of Camelot (DAOC, vive les abbréviations !) est beaucoup plus récent que les autres MMORPG cités auparavant (sorti il y a à peine un an aux USA). Il ne faut donc pas trop rêver, ce n'est pas tout de suite que vous pourrez vous passer des serveurs officiels... mais tous les espoirs sont permis puisque des projets sont en cours de développement.

1) Le jeu

DAOC fait partie, avec Anarchy Online, de la génération suivante de MMORPG. Comme entre EQ et UO, il y a donc un grand fossé technique entre DAOC et EQ. De plus, le background de DAOC fait preuve d'originalité, puisque son histoire se place aux temps des Chevaliers de la Table Ronde, ce qui apporte une certaine bouffée d'oxygène par rapport aux autres MMORPG. Les amateurs de culture celte que vous êtes apprécieront.

2) Les émulateurs

Aurais-je dû écrire " l'émulateur " ? Le fait est qu'aujourd'hui un seul émulateur est officiellement en développement : il y en a eu d'autres, mais ils ont disparu ou se sont regroupés entre eux, et maintenant il ne reste plus en lice que COADServer [30]. Au moins, il s'agit d'un projet sérieux et qui avance régulièrement. Par contre, la première version n'est pas encore sortie, et lorsqu'elle sortira, tout ce qu'on pourra faire dessus sera se déplacer et discuter (si tout va bien). Autant dire qu'il reste encore du temps avant de pouvoir vraiment s'éclater en ligne dessus.

3) Les Shards et les outils

Il n'y a pas d'émulateur, et vous voulez déjà des Shards ? Faut pas rêver, c'est pas pour demain ! Cependant, le site de United Gaming Project [31] a pour objectif de proposer des outils pour le développement sur DAOC, et leur premier projet est... un créateur de monde. Ce qui est bon signe pour la suite, puisqu'un tel outil est absolument nécessaire pour créer un Shard sérieux.

Et Anarchy Online dans tout ça ?

Malheureusement, tout ce que qu'il existe pour l'instant en terme d'émulateur pour Anarchy Online, ce sont des rumeurs. Et même, il n'y en n'a pas beaucoup. Donc si vous voulez un émulateur, le mieux à faire à mon avis, c'est de l'écrire vous même !

Et Star Wars Galaxies ? Et World of Warcraft ? Et ..... on verra ça dans un prochain numéro, d'accord ? ;)

Tous les liens :

[1] The Smithy's Anvil, la meilleure source de news sur l'émulation des MMORPG : http://www.smithysanvil.com/
[2] La Quatrième Prophétie, le plus grand MMORPG français gratuit : http://prophetie.goa.com/
[3] Epsilon, un émulateur pour UO : http://www.epsilon.escend.net/
[4] Legend Server, un émulateur pour UO : http://www.legendserver.com/
[5] LoneWolf, un émulateur pour UO: home1.tiscalinet.de/aduke/main2/news2.htm
[6] Nox Wizard, un émulateur pour UO : http://nox-wizard.sunsite.dk/site/
[7] POL, un émulateur pour UO : http://pol.tumbolia.org/
[8] Revelation, un émulateur pour UO : http://revelationemu.sourceforge.net/
[9] RunUO, un émulateur pour UO : http://www.runuo.com/
[10] Sphere, un émulateur pour UO : http://www.sphereserver.net/
[11] Tupi, un émulateur pour UO : http://tupi.sourceforge.net/index.php
[12] UOX3, un émulateur pour UO : http://www.uox3dev.net/
[13] UOX Classic, un émulateur pour UO : http://www.uoxclassic.com/
[14] Wolfpack, un émulateur pour UO : http://wpdev.sourceforge.net/
[15] UO Gateway, un outil pour se connecter automatiquement aux Shards UO : http://www.uogateway.com/
[16] La liste de Shards UO de Jeux Online, en français : uo.jeuxonline.info/liens/links.php?cat=17
[17] Ultima Online Top 200, une liste de Shards UO (essentiellement US) : www.gamesites200.com/ultimaonline/
[18] UO Rice, pour éliminer l'encryption des données : http://stud4.tuwien.ac.at/~e9425109/UO_RICE.htm
[19] Des Clients UO, si le vôtre ne fonctionne pas : http://www.angelfire.com/super/clients2/
[20] UOP, un client open source pour UO : http://uop.sourceforge.net/
[21]UO Auto-Map, pour ne plus se perdre dans UO : http://uoam.net/
[22] Inside UO, pour fouiller dans les données d'UO : http://dkbush.cable-net-va.com/alazane/insideuo_ss.html
[23] EQEmu, un émulateur pour EQ : http://www.eqemu.net/
[24] EthernalQuest, un émulateur pour EQ : http://www.hackersquest.org/
[25] EQWindows, pour jouer à EQ en mode fenêtré : http://eqw.eqhackers.com/
[26] ShowEQ, outil qui dévoile des informations supplémentaires au joueur d'EQ : http://seq.sourceforge.net/
[27] ACdome, l'actualité de l'émulation sur AC : http://www.acdome.com/
[28] UAS, un émulateur pour AC : http://uas.ath.cx/
[29] Third Party Paradise, tous les programmes utiles pour AC : http://acplugins.cjb.net/
[30] COADServer, un émulateur pour DAOC : http://www.coadserver.com/
[31] United Gaming Project, dédié à la création de Shards pour DAOC : http://www.ugproject.com/

Saddam a mail ouvert : hacking ou propagande ?

Brian McWilliams, journaliste vivant dans le New Hampshire, prétend avoir réussi à pénétrer dans la boîte aux lettres électronique du président irakien. C'est en se connectant à un site officiel irakien qu'il a fait sa découverte, après avoir tapé un mot de passe intuitivement. Entre juillet et août 2002, le dictateur Saddam a reçu plus de mille mails, mais apparemment personne ne les consulte. Parmi eux, des insultes, comme celles de ce parachutiste la Guerre du Golfe, ou des soutiens d'admirateurs autrichiens, prompts à critiquer l'impérialisme américain. Le journaliste a également découvert des propositions de discussions commerciales de la part d'une entreprise californienne, alors que l'Irak est sous embargo international !

game hacking

CREEZ VOS PROPRES CHEATS CODES

Votre jeu préféré est trop difficile, et il n'y a pas de cheat connu ? Nous allons vous apprendre à créer vous-même des trainers pour réussir à tricher sur tous les jeux.

GAMECUBE : ÇA BOUGE ENFIN UN PEU

Les rumeurs sur la GameCube vont bon train. Pour l'instant rien n'est vraiment sûr, et papi Mario rigole dans son coin à chaque fois qu'on apprend que non, c'était une blague, on ne peut pas encore copier les jeux sur GC. Cela dit, certaines rumeurs sont plus fondées que d'autres : ainsi, un groupe pirate (Kalisto) aurait pu copier un jeu. C'est bien possible. Par contre, pour l'instant il n'y a pas de modchips pour votre GC (ceux qu'on peut trouver sur le net sont des arnaques, attention). La seule console sur laquelle on pourrait éventuellement faire tourner une copie serait le modèle Q de Panasonic, qui est vendu en Asie. De toute manière, le jour où on pourra copier les jeux GC, ne vous inquiétez pas, on le saura vite ! Pour les émulateurs, c'est pareil : ne rêvez pas. Il en existe bien un à télécharger sur http://benjamin.francois.free.fr/artwork/gcubix/. Comment ça c'est un fake ? Vous n'y croyez pas, vous, qu'il tourne même sur GameBoy ? Tant pis, c'est pas grave, à part ça je connais quelqu'un qui connaît quelqu'un qui connaît quelqu'un qui a un émulateur GC qui marche !!! Si si, promis. Il ne veut pas dire où on peut le télécharger, par contre.

HOLD-UP SUR LES NOMS DE DOMAINE

Les internautes ont été virés de la direction de l'ICANN, l'organisme chargé de la gestion des noms de domaine sur Internet. Stuart Lynn, président de l'ICANN, justifie cette décision péremptoire par les critiques sur le fonctionnement de l'organisme. Mais comment croire que c'est en privant les internautes de leurs voix que l'ICANN va retrouver sa légitimité ?

QU'EST CE QU'UN TRAINER ?

Pour résumer, un Trainer (se prononce "traîneur") est un programme de triche qui tourne en arrière plan lorsque vous jouez au jeu pour lequel il est destiné. Il vous donne un "bonus" (armes, munitions, argent, vie, objets, points...) lorsque vous appuyez sur une touche spécifique, tout en restant dans le jeu. Pour cela il y a plusieurs moyens. Soit utiliser des combinaisons de caractères, créées la plupart du temps par les développeurs du jeu lui-même (= cheat codes), soit en modifiant les valeurs des zones mémoires spécifiques utilisées par le jeu (ce que l'on va faire).

Ce tutoriel est destiné aux débutants, il est donc inutile de le lire pour après râler en disant que le niveau est trop bas si vous avez déjà les bases.

RECHERCHE

Commençons dans l'ordre des choses, eh oui l'oeuf ne vient pas avant la poule, alors lançons-nous dans ce travail, certes ennuyeux et plutôt fastidieux, mais nécessaire. Soit vous êtes un paresseux irrécupérable et vous allez chercher les cheats codes sur un site spécialisé, ou encore étudiez le fonctionnement d'un trainer déjà mis au point (lame), soit vous êtes un puriste et vous continuez votre (passionnante :P) lecture.

Nous allons commencer en douceur en essayant de tricher à ... *roulements de tambour* ... *roulements de tambour* ... PacMania3D ! Ce shareware est disponible en téléchargement sur le site de son auteur : (http://www.alawar.com/games/pacmania3d/)

Et comme outil, nous allons prendre MemHack, qui est léger, simple et efficace. Vous pouvez le télécharger sur le site officiel (http://www.memhack.com).

KAY ? LET'S GO !

Lancez PacMania, puis MemHack, et sélectionnez "PacMania3D" dans "Running processes". Maintenant jouez un peu, puis arrêtez-vous après avoir avalé quelques-unes de ces étranges boules blanches dont la composition chimique reste un vrai mystère pour le monde scientifique...

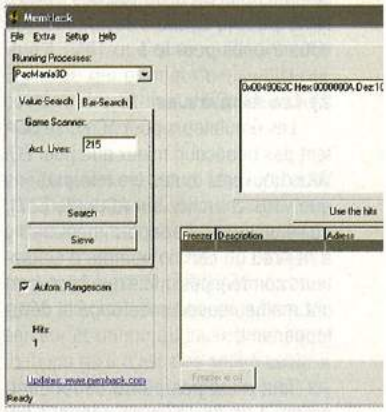
Appuyez sur Echap pour faire pause et retournez dans MemHack. Décochez "Autom. Rangescan", puis mettez votre score dans "Act. Lives :" (pour moi c'est 205) et cliquez sur "Search". Ne vous inquiétez pas si la recherche est un peu longue...

Vous devriez observer quelque-chose de ce genre :

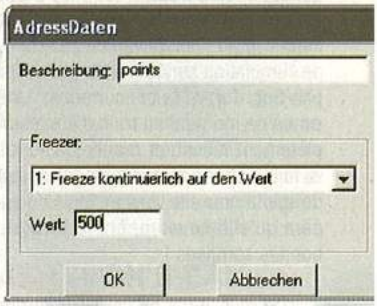
```
Scanning Memory: xxx
Scanning Memory: xxx
Scanning Memory: xxx
[...]
Ready
```

OK ? On est sur la bonne voie, mais il y a malheureusement trop de réponses, alors retournez dans le jeu et continuez à gober ces délicieuses boules blanches, puis retournez dans MemHack afin de chercher votre nouveau score (215 pour moi), mais maintenant, vous allez cliquer sur "Sieve " et non "Search".

Résultat : "Hits : 1" ! BINGO ! On la tient enfin cette fameuse adresse

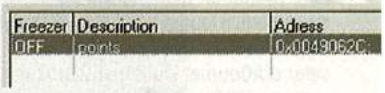


Maintenant cliquez sur "Use the hits" :

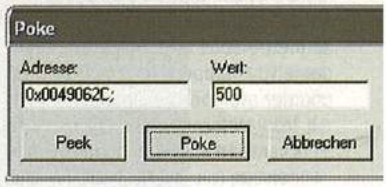


Pour ceux qui ne comprennent pas l'Allemand :
"Beschreibung" = description (facultative)
"Wert" = valeur.

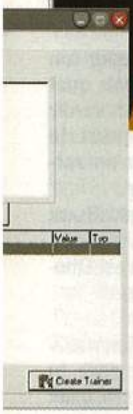
Entrez 500 par exemple, puis validez. Vous obtenez ceci :



Cliquez droit sur cette ligne, puis cliquez sur "Peek & Poke" :



Maintenant cliquez sur "Poke" et retournez dans le jeu...



Et voilà ! Nous avons nos 500 points durement gagnés ^_^

Note : Ce n'est pas grave si vous obtenez plusieurs adresses, le tout est de ne pas en avoir 10000 :)

Programmation

Le moment crucial est arrivé. La création du trainer ... *roulements de tambour* ... ("oh $@*&% il va pas recommencer ça !") ... Serez-vous capable de programmer un trainer pour exploiter ce que vous venez de découvrir !? *roulements de tambour* ... Nan bon, je rigole, mais c'est tout de même une partie délicate et souvent difficile à assimiler, enfin tout dépend de votre position par rapport à la programmation.

Si vous êtes débutant (Newbie Game Hacker) et que vous ne savez donc pas programmer, vous pouvez toujours utiliser le créateur de trainer intégré dans MemHack (voir la photo d'écran ci-dessous).

Bon ok, c'est pas le top mais c'est toujours mieux que rien, surtout si vous voulez absolument distribuer vos trainers.

Value	Typ
500	1

Pour les autres, je vais vous faire un petit exemple (toujours pour PacMania3D) pour avoir des points lorsqu'on presse CRTL+F1 pendant une partie avec Delphi.

Pour cela, nous allons utiliser les API (Application Programming Interface) suivantes :

// Pour détecter les touches pressées :
GetAsyncKeyState(virtual-key code);
// Pour trouver la fenêtre du jeu :
FindWindow(address of class name, address of window name);
// Pour récupérer l'ID :
GetWindowThreadProcessId(handle of window, address of variable for process identifier);
// Pour ouvrir le processus :
OpenProcess(access flag, handle inheritance flag, process identifier);
// Pour écrire dans la mémoire :
WriteProcessMemory(handle of process whose memory is written to, address to start writing to, address of buffer to write data to, number of bytes to write, actual number of bytes written);
// Pour fermer l'handle :
CloseHandle(handle of object to close) ;

IV - Conclusion

Bon bah voilà, c'est déjà terminé... Si vous avez une question intelligente, une remarque, ou quoi que ce soit d'intéressant, envoyez-nous un mail !

Écrit par Majen.

Liens

vngamecenter.com
membres.lycos.fr/tsearch
geocities.com/smil0r26
www.trainerscity.com
www.gamehacking.com
www.extalia.com

Begin Code

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms, Dialogs, StdCtrls, ExtCtrls;

type
  TForm1 = class(TForm)
    Timer1: TTimer;
    procedure FormCreate(Sender: TObject);
    procedure Timer1Timer(Sender: TObject);

  private
    { Private declarations }
  public
    { Public declarations }
  end;

// Variables

var
  Form1 : TForm1;
  Bchr  : pchar;
  Fentr : integer;
  PrcID : integer;
  ProID : integer;
  Opnpr : integer;
  Wrtpr : cardinal;

implementation

{$R *.dfm}


procedure TForm1.FormCreate(Sender: TObject);
begin
  Timer1.Interval := 1;                          // Définit l'intervalle à 1 milliseconde
  Timer1.Enabled  := True;                       // Lance le timer...
end;

procedure TForm1.Timer1Timer(Sender: TObject);
begin
// Si l'utilisateur presse CTRL+F1...
if (GetAsyncKeyState(VK_F1) <> 0) and (GetAsyncKeyState(VK_CONTROL) <> 0)
then
 begin
  Fentr := FindWindow(nil,'PacMania3D');         // On cherche la fenêtre
  PrcID := GetWindowThreadProcessId(Fentr,@ProID); // On cherche l'ID une fois
                                                   que la fenêtre a été trouvée
  Opnpr := OpenProcess(PROCESS_ALL_ACCESS,False,ProID);
                                                 // On ouvre le processus
  GetMem(Bchr,1);
// Pointeur...
  Bchr^ := Chr($10000);                          // Notre valeur (10000)
  WriteProcessMemory(Opnpr,ptr($0049062C),Bchr,2,Wrtpr);
                                                 // On écrit la valeur à
                                                    l'adresse 0049062C
  FreeMem(Bchr);                                 // On libère les ressources
  closehandle(Opnpr);                            // Et on ferme l'handle...
end;
end;

end.
```

End Code

Et voilà, c'est tout pour le code ! Pas si difficile que ça finalement, non ?

Fraude à la CB : La BNP mauvaise joueuse

La banque est au centre d'une affaire inédite : le tribunal de commerce d'Angers doit trancher sur la question de la responsabilité en cas d'escroquerie à la carte bleue sur Internet. Le responsable d'un site Internet de vente par correspondance s'est fait rouler au printemps 2002 par un prétendu industriel ivoirien qui lui achète des ordinateurs portables pour un montant total de 295 000 euros. Les paiements sont fractionnés et effectués de cartes bleues différentes. Mi-août, la BNP découvre que les cartes sont fausses ou volées et débite le compte du gérant afin de se rembourser. Le vendeur a-t-il respecté les règles de vigilance ? Ou la banque doit-elle faire jouer sa garantie ? Délibéré le 22 janvier 2003. En attendant, l'escroc s'en sort à bon compte, lui...

COURRIER DES LECTEURS

XBCONNECT CONCURRENCE XBOX LIVE

Certes, Microsoft a lancé à grand renfort de publicité son service de jeu online Xbox Live. Mais est-il vraiment besoin de payer 50 euros et d'enlever son modchip pour jouer en ligne ? Pas forcément. En effet, les jeux jouables en ligne sont aussi souvent ceux pour lesquels il existe un mode de jeu en réseau. Et, comme on vous l'explique pour Warcraft III dans ce numéro, il est souvent possible de faire croire à un jeu qu'il se connecte en réseau local sur une autre machine alors que celle-ci est quelque part sur internet ! C'est ainsi que Halo a pu être joué en ligne bien avant le lancement de Xbox Live. Dorénavant, d'autres jeux sont même supportés : la série des Tony Hawk, Nascar 2002, Moto GP, Serious Sam, Ghost Recon, Unreal Championship, ... Tout ça sur www.xbconnect.com/. Par contre, attendez vous à voir bien plus d'Américains que d'Européens, d'où des problèmes de lag.

FAIRE TOURNER SES VIEUX JEUX SOUS WINDOWS

Si vous êtes un fan de vieux jeux DOS, vous aurez remarqué qu'un des plus gros problèmes que l'on rencontre en voulant y jouer sous Windows est celui de la compatibilité de la carte son. Souvent, le jeu ne détecte pas correctement la carte, et vous aurez droit soit au silence complet, soit aux merveilleux gazouillis du haut-parleur interne du PC. Pour les possesseurs de Windows NT4, 2000 et XP, il existe heureusement une solution : VDMSound émule une carte son Sound-Blaster tout ce qu'il y a de plus compatible, ce qui devrait redonner de la voix à la plupart de vos jeux. Il existe d'autres cartes émulées, ainsi que d'autres options pour vous aider à faire tourner correctement les vieux hits. Tout ça sur http://ntvdm.cjb.net/

FAIT INSOLITE, IL Y A POUR UNE FOIS DU COURRIER DES LECTEURS DANS UN NUMÉRO 1 ! Il s'agit en fait du courrier concernant le dernier Pirat'gamez (le prédécesseur de Pirat'z), donc ça tourne plutôt autour des jeux. On attend vos remarques, suggestions, questions et autres sur notre mail qui reste pour l'instant : piratgamez@yahoo.fr. Au fait, il est inutile de perdre votre temps à nous demander où télécharger des jeux, ou tout autre genre d'adresse illégale, nous ne le savons pas.

Salut j'ai lu le numéro 4 de pirat'gamez où vous parlez de l'émulation. Je voudrais avoir plus de précision sur l'émulateur playstation (est-il vraiment fiable et fonctionne-t-il vraiment avec tous les jeux psx, peut-on faire tourner des jeux copiés ou seulement les originaux), sinon je voudrais savoir aussi ce que vous voulez dire par patches et trainers. Merci de m'éclairer @+

REDEMPTEUR

Non, on ne peut pas dire que ePSXe soit complètement fiable. Il reste des jeux qui vont tourner imparfaitement (graphisme ou son dégradé dans certaines séquences par ex.) ou qui ne vont pas tourner du tout. Tu peux trouver sur le net des listes de compatibilité comme ici : http://www.ngemu.com/compat/index.php?console=psx

Si tu en veux d'autres, cherche sur google "epsxe" et "compatibility" (+ éventuellement le nom d'un jeu en particulier). A part ça, les copies fonctionnent avec cet émulateur.

Un patch est un programme qui modifie un jeu. Sur ordinateur, un patch est une mise à jour du jeu (qui corrige des bugs par ex.), et est fourni par les développeurs du jeu. Sur console, on parle de patches pour les modifications du jeu qui permettent de contourner la protection par exemple : ce sont des fichiers non officiels qui sont créés par des crackers. Pour appliquer un tel patch, il faut convertir le jeu sous forme de fichier d'image disque, y appliquer le patch puis regraver le jeu.

Un trainer, c'est un programme qui permet de tricher dans un jeu. Sur console, on applique un trainer comme un patch. Ensuite, il y a généralement au démarrage du jeu un nouveau menu qui permet de sélectionner des options comme

énergie infinie, choix du niveau, ...

Voilà, si tu as du mal à voir exactement ce que c'est, tu n'as qu'à en essayer un toi-même !

Bonjour je vous écris pour savoir s'il y a des outils pour créer soi-même ses jeux de gameBoy et de Nintendo64 et les mettre sur des disquettes (de gameBoy et de Nintendo64). Si OUI pourriez vous m'envoyer les adresses des sites.

JEAN-EUDES

Oui il est possible de créer soi-même des jeux GameBoy ou N64. Cela dit, les mettre ensuite sur cartouche pour les utiliser nécessite un matériel assez cher et pas évident à trouver (car c'est avec le même genre de matériel qu'on peut copier les jeux, ce qui ne plait pas à Nintendo).
Pour la GameBoy, je te conseille http://www.devrs.com/gb/
Pour la Nintendo64, le site de Dextrose : http://www.dextrose.com/
Bon courage, car créer soi-même des jeux sur console n'est pas une mince affaire !

Salut ! J'espère ke vous allez bien les pirat' :p J'ai une kestion à vous demander : eske vous pouvez me dire le nom d'1 des meilleurs antivirus en francais si possible et où le télécharger en version complète ça serait gentil @+ merci

HAKIM LEBOSS

Désolé mais les meilleurs antivirus sont payants... il en existe quelques-un gratuits mais rarement en français :
http://www.secuser.com/antivirus/ : antivirus en ligne, explications en français
http://www.clubic.com/t/gen/fl2438.html : gratuit mais en anglais
http://www.grisoft.com/html/us_downl.htm : gratuit mais en anglais

Sinon, parmi les payants, des antivirus comme Sophos, Norton AV ou Panda AV sont dispos en VF.

Tout d'abord félicitations pour ton magazine. Je voudrais savoir quel logiciel il fo utiliser pour savoir qu'est ce qui sort par les ports. Je voudrais essayer d'émuler un serveur de la 4éme Prophetie.

SIRIUSBLACK

Le meilleur outil à utiliser est Ethereal, à télécharger sur :

http://www.ethereal.com/distribution/win32/
Lis les instructions sur cette page, tu noteras qu'il faut également installer WinPcap, dispo sur :
http://winpcap.polito.it/install/default.htm
Bon courage pour émuler un serveur, il s'agit d'un boulot pas évident du tout !

J'ai acheté votre journal parce'que il y avait un titre attrayant "100% ruse". Et bien je suis déçu puisque ce que vous publiez sur du papier basse qualité et vendez à un prix super fort, n'a rien de sensationnel. Merci de me répondre.

ANDREI T.

Il est très difficile de plaire à tout le monde. Les courriers reçus étant dans la très grande majorité positifs, je pense que notre ancienne formule plaisait à la majorité. Espérons que la nouvelle (prix inférieur à 10 francs, papier glacé, et deux fois plus de contenu) permettra de satisfaire les plus exigeants comme toi :)

J'ai découvert récemment un nouveau logiciel de gravage que je trouve particulièrement bien pour tout graver. Il s'agit de BLINDWRITE et je suis surpris que vous n'en parlez pas dans vos MAGS.

JEAN CLAUDE L.

BlindWrite, c'est un peu comme CloneCD, mais en un peu moins puissant. Cela dit, il a déjà rattrapé pas mal de son retard et c'est vrai qu'il mérite qu'on le cite. Voilà qui est fait :) A télécharger sur http://www.blindwrite.com/

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. Articles du code de la propriété intellectuelle relatifs aux logiciels, parce que nul n'est censé l'ignorer : 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 plateformes : www.megagames.com
GameCopyWorld. Cracks et utilitaires pour faciliter la sauvegarde : www.gamecopyworld.com

-Copie (gravure, modchips, ...)

Files Forums. Forums dédiés à la sauvegarde et à la gravure : www.fileforums.com
CD Media World. Tout sur la gravure : utilitaires, articles, tests, ... : www.cdmediaworld.com
Ominfo. Un forum français fort instructif pour les consoles : www.ominfo.com/forum/

-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 NEWS

-Web

iSONEWS. La référence de l'actualité warez : 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

P2PFr.com. Un portail français sur le P2P : p2pfr.com
Ratatium. Un autre site français couvrant l'actualité : www.ratiatum.com
Direct Connect. Logiciel de partage P2P original : www.neo-modus.com
EDonkey. Logiciel de partage P2P : www.edonkey2000.com
Open-Files. Un site français sur eDonkey, eMule et Overnet : www.open-files.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.abandongames.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

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 sympa en français : www.toudy.com

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 : www.pvpgn.org

CHEATS

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
GameThreat.com. Présentation d'outils de cheats sur PC : www.gamethreat.com/tools/
PEC. L'outil ultime pour tricher sur émulateurs PSX : www.emucheater.com

FLICAGE POUR COLLÉGIENS VAROIS

Un collège du Var a mis en place un système bien particulier pour permettre à ses élèves d'accéder à la cantine : les jeunes seront reconnus par leur main ! Ils devront composer sur un clavier un code personnel à trois chiffres, puis glisser leur main dans un boîtier électronique muni de " tétons capteurs " qui reconnaîtront précisément la main, ses contours et son épaisseur. Sans ça, le petit ne pourra pas aller manger. Ce même collège a installé un système de SMS pour prévenir les parents en cas d'absence. Big brother is watching you...

LES "REBELS" S'EXPOSENT À NYC

L'exposition "Illegal Art" s'est ouverte à New-York. Divertissante et provocante, l'exposition se compose d'images médiatiques volées et recomposées par des artistes, parfois poursuivis en justice pour de tels usages. Résultat : le programme est alléchant, à consulter en direct sur www.illegal-art.org.

VIRUS FACTORY

Virus writers, ne vous cachez plus !

Fabriquer un virus, c'est si simple ! Des outils pirates, librement téléchargeables sur le Net, mettent la création des virus informatiques à la portée du premier venu. Pirat'Z vous dit tout.

Première constatation : les auteurs de virus ne se cachent pas. Mais comment s'en étonner, puisque leur passion consiste justement à exposer et à diffuser le plus largement possible leurs " œuvres " ? Dans les dix premiers résultats de notre recherche sur google.com, avec les mots clés "virus creation", se trouve le gros lot. Ce site public et accessible à tous, très bien référencé dans les moteurs de recherche, se revendique comme étant le paradis des virus. Il possède de plus de 500 méga octets de magazines électroniques, de codes sources de virus, et de tutoriaux divers. Sans parler des 7128 virus au format exécutable, directement prêts à être téléchargés et lancés sur Internet. Effrayant.

(sans doute la dernière puisqu'elle ne sera plus maintenue), elle comporte une centaine de ces infâmes programmes, qui sont à peu près tous fonctionnels. Notre photo d'écran de VDAT montre la diversité des logiciels disponibles : depuis les virus pour DOS/Windows 3.1 jusqu'à Windows 2000, en passant par les macro-virus qui attaquent la suite Office de Microsoft. On pense qu'il est important de connaître ces techniques pour être au courant des dangers encourus sur Internet. On va donc vous présenter, pour votre information, quelques kits de création de virus parmi les plus connus. Ce sont aussi les plus anciens. Sachez qu'il existe sur les mêmes sites web des outils de création de virus mis à jour et encore plus dangereux !

La philosophie des virus writers se base sur le droit à la connaissance et à la liberté d'expression. Oui, il est illégal d'attaquer des systèmes, donc de diffuser des virus sur Internet. Mais aucune loi n'interdit en France la création et la diffusion des savoirs et des codes sources permettant de réaliser des virus, ou de contourner des protections. Sur sa page de garde, le site contenant la plus grosse base d'archives de virus rappelle l'article 19 de la déclaration des Droits de l'Homme : " Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit. "

Mais le pire, ce sont les kits de construction de virus. Ces véritables boîtes à outils permettent de créer ses propres virus personnalisés à l'aide d'une souris, d'un demi-neurone, et d'un pack de bières (optionnel). Sur le net, on trouvera ainsi la base VDAT. C'est une grosse archive de virus et de tutoriaux, compactés par Cicatrix dans un seul fichier... exécutable (avec ou sans virus ? on ne sait pas !). Actuellement dans sa version 1.8

Word 97 Macro Virii Creation Kit

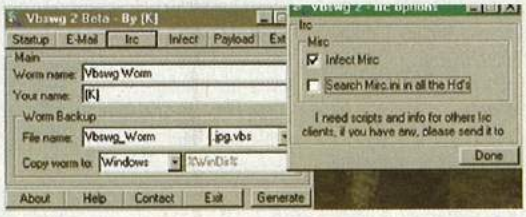
von Jack Twoflower!Lz9 Vx Team

Comment créer un virus pour Word ? Il faut l'écrire en langage Visual Basic, au sein de macros. Nous avons testé le prog " Word 97 MacroVirii Creation Kit ", qui devrait être aussi compatible avec Word 2000. Cet outil peut être exécuté directement en cliquant sur l'icône associée dans la base VDAT. Et nous le confirmons : ça marche ! Nous avons pu créer un document Word contenant notre virus au sein de la macro Autopen(). Mais nous aurions aussi pu aussi utiliser un outil pour créer un code polymorphique crypté évitant la détection par certains antivirus.

Vous vous rappelez d'Anna Kournikova ? Ce ver qui a causé des millions de dollars de dégâts était un simple script vbs généré par un kit comme celui que nous avons testé. Il s'agit de WBSG : possibilité d'infecter le client irc MIRC, de se reproduire par e-mail via le carnet d'adresse Outlook, de s'auto-crypter et d'empêcher la suppression du virus quand celui est installé sur le disque. On peut aussi y adjoindre un fichier exécutable (par exemple un cheval de Troie pour contrôler l'ordinateur à distance) qui s'exécutera automatiquement sur les machines infectées. Le code source du virus ainsi généré peut être ensuite lu et éventuellement modifié à la main.

Pourtant, dans le kit de virus pour Word, l'auteur a prévu des lignes de code pour détruire les antivirus présents sur la machine attaquée... Bien sûr, si votre antivirus est à jour, il aura détecté et bloqué ce virus avant même son exécution... mais le code source du kit de construction pourrait facilement être modifié par un internaute mal intentionné qui connaît le langage Basic. Les nouveaux virus ainsi créés seront un peu différents, et ne seront donc pas reconnus par les antivirus, du moins pendant un certain laps de temps. Si vous récupérez, d'une façon ou d'une autre, un fichier infecté de cette manière, vous n'avez donc absolument aucun moyen de vous protéger ! Les filtres de contenu web comme e-safe c'est bien, mais ça ne suffit pas si vous cliquez sur n'importe quoi. Alors faites bien attention à ce que vous téléchargez sur le Net...

PROTECTION IMPOSSIBLE



On vous conseille d'installer un bon anti-virus, par exemple la version gratuite d'AVG, disponible sur http://www.grisoft.com/html/us_downl.htm#FREE. Et surtout, pensez à faire les mises à jour régulièrement par Internet, de préférence plusieurs fois par semaine.

PIRAT'Z HACKERS & GAMERS

L 19302 - 7 - F: 1,50 € - RD