N°4 AOÛT - SEPTEMBRE FULL PIRATAGE SUR 32 PAGES SANS PUB

PIRAT'Z

HACKERS & GAMERS

1 Même pas dix balles !! 1,5 €

L 19302 - 10 - F: 1,50 € - RD

PIRAT'Z - PIRAT'Z - PIRAT'Z - PIRAT'Z - PIRAT'Z - PIRAT'Z

LECHATKITL

ANONYMAT : Invisible partout sur le Net

WAREZ News • MAILBOMBING en Puissance

LINUX ou WINDOWS ? • MODCHIPS PS2

HACKING XBOX • FAILLES Boutiques • CRACKING

ET TOUTES LES VULNÉRABILITÉS LES PLUS HOT

EDITO

Aaaah, voici l'été, ses magazines d'informatique bien remplis et ses heures perdues en vacances à St-Trou-du-Poirier au bord de la plage, quand on pourrait être tranquille devant son écran d'ordinateur sans craindre les coups de soleil... Enfin, moi je dis ça, mais aussi bien c'est déjà la rentrée au moment où vous me lisez, et vous aimeriez bien y retourner à St-Truc-du-Pommier. Oups. Mais quoi qu'il en soit, réjouissez-vous, vous tenez dans la main un nouveau numéro de Pirat'z, rempli à craquer comme il se doit (si vous avez des doutes, demandez à notre maquettiste, il en fait encore des cauchemars). Vous avez été plusieurs à vouloir savoir comment être anonymes sur le net. Vous trouverez donc un gros dossier comme on les aime sur le sujet, qui ne prétend pas être exhaustif mais devrait vous donner un bon point de départ. Et puis comme ça vous pourrez nous envoyer des emails anonymes - oups des courriels anonymes je veux dire - puisque certains d'entre vous sont encore trop timides pour nous écrire. Il y en a aussi par contre qui ne sont pas assez timides, ils se reconnaîtront ;-) Mais non, c'est une blague, on les aime tous nos lecteurs. C'est quand même grâce à vous qu'on loge au Ritz et pas dans le caniveau. Oh, excusez-moi... "oui, le champagne avec le caviar, s'il vous plaît". Désolé, c'est que ce n'est pas facile tous les jours ici, comme vous pouvez le voir ! En plus, ils n'ont toujours pas d'abonnement à Pirat'z, je dois aller l'acheter moi-même chez le marchand de journaux. Quelle honte ! Enfin, je parle je parle, et voilà encore un édito tout décousu, on dirait presque que je l'ai écrit à 2h du matin la veille du bouclage. Heureusement que personne ne me lit. Enfin j'espère.

Khan
tiho@netcourrier.com

PIRAT'Z
HACKERS & GAMERS

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

Directeur de Publication : Olivier André
Rédacteur en chef : Khan
Conception Graphique : 02prod
Illustrations : Lechatkitu, yok2003
Imprimé en CE

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

SOMMAIRE

INTERNET EXPLORER FAIT UNE PAUSE

Microsoft a annoncé qu'il n'y aurait plus de nouvelle version d'Internet Explorer. Plus précisément, "en tant que composant du système d'exploitation, IE continuera d'évoluer, mais il n'y aura pas d'autre version indépendante". Comprenez par là que Microsoft va quand même devoir continuer à corriger les bugs restant dans IE6 SP1 pendant encore longtemps, mais qu'ils renoncent à en rajouter encore en sortant une version 7. C'est une triste nouvelle pour les fans d'IE, mais on s'en fout car ceux-ci se réduisent à Billou, Stevie et Nicolas, 3 ans. Plus intéressant est de savoir comment va évoluer le marché des navigateurs, puisque les concurrents vont avoir enfin le temps de rattraper leur retard. C'est mal parti pour Netscape, puisqu'AOL (qui l'avait racheté il y quelques temps) semble plus le considérer comme un cadavre puant dont il faudrait mieux se débarrasser que comme un futur produit phare. Restent donc Opéra (s'il veut bien enlever ses pubs), Mozilla (s'il veut bien enlever ses bugs), mais surtout Lynx (lynx.browser.org). Euh, après tout, je veux IE7!!!

LE PEERCACHE, UNE BELLE IDÉE EMBARRASSANTE

À la mi-juillet, trois des plus gros FAI européens ont acheté la licence de PeerCache de JoltID (ils ont souhaité garder l'anonymat). Les FAI sont protégés par la loi des droits d'auteur aux États-Unis, mais le PeerCache les met pour le moins dans l'eau bouillante puisque ce logiciel stocke des logiciels (films, musiques et autres) dans les serveurs des FAI et par là-même les rend plus accessibles. L'IFPI (représentant mondial de l'industrie du disque) déclare que ce que fait JoltID et leurs clients est loin d'être très clair, mais qu'ils tenteront d'éclaircir tout ça avant de prendre des mesures. Le directeur de JoltID se défend en s'appuyant sur une loi de l'Union Européenne, qui permet aux FAI de stocker le trafic sur leurs serveurs, sur une courte durée, sans qu'ils aient à en vérifier toute la légalité. Il ajoute que les FAI ne sont pas là pour encourager ni décourager les partageurs de P2P, mais seulement pour réduire le trafic internet. En tout cas, c'est bien joué de la part de JoltID qui se fait ainsi des sous sur le dos des majors!

SI MICROSOFT FAISAIT DES VOITURES...

De nombreuses blagues commencent ainsi, avec différentes versions pour la fin, comme "l'airbag vous demanderait 'Etes-vous sûr?' avant de se gonfler". Et bien, ne riez pas trop, car MS fait effectivement des logiciels pour voitures. D'ailleurs, une mésaventure est arrivée à un ministre thaïlandais: il est resté coincé à cause d'un bug de l'ordinateur de bord qui a bloqué les portes et stoppé l'air conditionné, et les gardes ont dû défoncer la limousine. Le logiciel contenait (entre autres) du code de Microsoft. Avait-il oublié de patcher?

RIEN QUE POUR VOS YEUX

Ca ne vous est jamais arrivé, d'entendre votre mère vous gronder? "Ca fait des heures que tu joues, tu vas t'abîmer les yeux!". Maintenant, vous pourrez lui répondre: "mais pas du tout maman, au contraire, d'ailleurs c'est marqué dans Pirat'z!" (et tout le monde connaît le sérieux de Pirat'z (euh (bon, bref)). Toujours est-il qu'une recherche scientifique (si si) a montré que jouer à des jeux vidéo permettait d'augmenter son acuité visuelle. En plus, vous avez de la chance, ça marche mieux avec Medal of Honor qu'avec Tetris.

LE BIEN CONTRE LE MAL

Les studios de films américains se lancent dans une campagne anti-piratage. La façon de procéder : le demander gentiment. La MPAA a développé une sorte d'historique sur le droit d'auteur qui sera enseigné dans certains programmes d'études. Le programme "Digital Citizenship" se terminera par un concours à l'échelle des États-Unis. Les étudiants suggéreront des moyens de convaincre les partageurs que télécharger des films, ce n'est pas seulement illégal, mais MAL. Nous connaissons tous les Américains, et savons que le bien et le mal leur ont toujours fait vendre des films souvent plus mauvais les uns que les autres. Selon un dirigeant de News Corp., "il ne s'agit pas d'attirer la sympathie de la part des gens, mais il faut avoir du respect pour les créateurs de ces films, ce n'est pas juste une question d'argent". Ces pauvres créateurs doivent sans doute être sur le bord de la faillite à cause des utilisateurs de P2P...ces derniers représentent évidemment le mal et les premiers, on l'aura deviné, le bien... Vous pariez que Yoda nous fera la morale dans l'Episode 3?

ADIEU FAIRLIGHT

La journée du 6 juin dernier a été marquée par le retrait de la Scène Warez du fameux groupe Fairlight. Une nouvelle accueillie tristement par leurs nombreux fans, qui se sont exclamés "That sucks !", avant d'aller télécharger COLIN.MCRAE.RALLY.3-DEViANCE. Mais soyons un peu moins chiens à Pirat'z : ce groupe mérite bien une petite page en guise d'adieu.

L'annonce du retrait du groupe s'est faite d'une manière toute particulière : le groupe a sorti un "jeu" dont le répertoire était intitulé Fairlight_Farewell-FLT, contenant un unique fichier flt-ff.nfo que voici :


```
                                                    ANSi·JED<ACiD>

      In Their 16th Year Of Glory, FairLight Released

                          Fairlight Farewell

:  Supplied by: FAIRLIGHT          : : Release Date: 6/9/2003        :
   Cracked by:  FAIRLIGHT              Game Type: Adventure
   Packaged by: FAIRLIGHT              Image Format: NFO

   CDS: 1                              Protection: None
   CD1 archives: 1  x 15 MB            CD1: flt-ff.nfo

  System Requirements: PC

Information :
=============

It has been a good few years, but it is now time for Fairlight to close its
doors for good. Many reasons have made us come to this judgement but we feel it
is for the best. The scene is getting to be a dangerous place. Not only do we
have to fear from the feds but also the unhonorable ones in the scene who lower
themselves to narq the competition. Retiring on top seems to be the best
decision for us. We want to thank all those throughout the years who have helped
us in one way or another.

                                                       /Team FairLight

Greetings to our friends in groups such as:
-------------------------------------------
CLASS, STN, KALISTO, ECHELON

                  +-+  QUALITY, TRADITION  AND PRIDE +-+

[ ------------------------------------------------------------------- ]
[  +++  (:  * <<< Hoopy's Topsite Scripts v3.00 for glFTPd >>>  *  :)  +++  ]
[ ------------------------------------------------------------------- ]
```

Le groupe a donc décidé d'arrêter son aventure à cause des trop grands risques encourus au niveau légal. Depuis décembre 2001 et le démantèlement du groupe DrinkOrDie, il y a eu en effet d'autres opérations anti-pirates ayant abouti à l'arrestation de membres importants de la Scène, même si elles ont été moins médiatisées. Comme il est souligné dans ce NFO, les groupes ne doivent pas seulement se protéger contre les attaques extérieures : la menace est aussi interne, avec des membres de la Scène travaillant comme "espions" pour les autorités. Ces derniers sont appelés des "Narqs", et sont évidemment détestés autant qu'ils sont redoutés par leurs "compagnons" de piratage. Bref, Fairlight a estimé que les risques n'en valaient plus la peine, ce qui se comprend bien quand on connaît les sentences infligées à certains membres de DrinkOrDie (quelques années en prison) ou Razor1911 (un ancien leader vient justement d'en prendre pour 18 mois) : c'est cher payé pour un passe-temps !

La disparition de Fairlight risque de modifier le paysage des groupes pirates sur PC. En effet, Fairlight était peut-être le plus fameux et le plus respecté des groupes, au top de la compétition depuis plus de dix ans. Les deux autres principaux groupes concurrents (Razor1911 et Deviance, enfin surtout Deviance depuis un certain temps) lui emboîteront-ils le pas ? Apparemment non, en tout cas pas pour l'instant. Finalement, ce qui devrait être considéré comme une bonne nouvelle pour les éditeurs de jeux (un groupe pirate de moins) pourrait bien donner l'effet inverse de celui escompté : Fairlight parti, voilà un peu de place pour d'autres groupes moins connus. Ainsi, le groupe Immersion sort de plus en plus de jeux (le dernier Flight Simulator 2004 par exemple), et d'autres groupes sortent des jeux qu'ils n'auraient peut-être pas pu sortir si Fairlight avait été là. Par exemple, coïncidence assez surprenante, le groupe "Game", quasi inconnu jusqu'à présent, a sorti le jeu "Pirates of the Caribbean", un gros titre de Bethesda Software... dont la dernière extension à Morrowind, Bloodmoon, avait justement été crackée par Fairlight le 4 juin ! Je vous laisse en tirer vos propres conclusions, mais on peut supposer que certains membres du groupe traînent encore dans les parages... Les internautes qui ne peuvent se passer de leur ration quotidienne de jeux piratés n'ont donc pas à trop s'inquiéter, la relève est là.

Il n'empêche, voir un groupe aussi prestigieux que Fairlight s'arrêter pour de telles raisons met en question le futur de la Scène. Parviendra-t-elle à renforcer ses mesures de sécurité et à résister aux assauts dont elle est l'objet, ou est-elle aujourd'hui à l'aube de son déclin ? Nul ne le sait, et tout le monde s'en fout après tout, mais ça fait toujours bien une conclusion un peu mélodramatique. Dont acte.

'Z

LES QUATRE ÉTAPES DE BASE POUR PÉNÉTRER LA PLUPART DES SYSTÈMES

Toutes les façons de pénétrer un système de sécurité sont différentes et tout dépend des habiletés de "l'attaquant" et des moyens de protection de votre ordinateur. Toutefois, la plupart de pirates suivent les mêmes quatre étapes de base pour y arriver: ils créent le profil du système, scannent, explorent et exploitent. Il n'est donc pas étonnant que le scan soit si mal vu, même si cette activité est en elle-même inoffensive. La première étape consiste à trouver le plus d'informations possible au sujet de la structure du réseau informatique, on peut par exemple trouver ses renseignements sur Internet (WHOIS). Les coordonnées telles que le numéro de téléphone ou le mail des dirigeants ou des agents techniques sont offerts par certains sites et l'e-mail est souvent la porte d'entrée du système (sendmail a généreusement fait parler de lui il y a peu avec une belle vulnérabilité). Il est ainsi possible de trouver les adresses IP et autres renseignements dont les hackers ont besoin. Et le tour est joué, il ne reste "plus" qu'à hacker!

LES AVENTURES DE LA RIAA... LA SUITE

La croisade de la RIAA contre les personnes téléchargeant des mp3 se poursuit. En effet, le président Cary Sherman déclare que l'association débute plusieurs centaines de poursuites, et selon celui-ci ce ne serait que le début. La RIAA n'est pas au bout de ses peines puisque les logiciels de P2P promouvant l'anonymat se succèdent (EarthStation5 et co, voir article anonymat de ce numéro). ce qui rend la tâche plus difficile pour la RIAA. A vous de faire votre choix... personne n'avait donc remarqué que Kazaa rimait avec RIAA?

MAILBOMBING MODE D'EMPLOI

Un sympathique lecteur souhaitant faire une petite blague innocente à un de ses amis nous a réclamé un tutorial sur le mailbombing. Et bien en voici donc un, il suffisait de le demander !

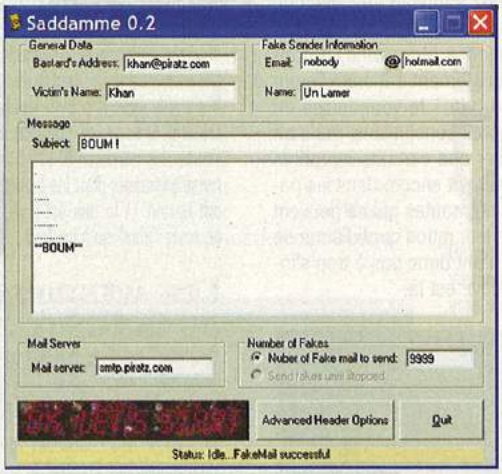
Le mailbombing consiste à essayer de faire "exploser" une boîte aux lettres en y envoyant une grande quantité de mails, de manière à la saturer et empêcher l'utilisateur de lire et recevoir correctement ses courriers. Evidemment, ce n'est pas une activité très recommandable, donc attention :

N'ENVOYEZ PAS UNE GRANDE QUANTITE D'EMAILS NON SOLLICITES, VOUS RISQUEZ DES ENNUIS. En effet, si la victime se plaint auprès de votre fournisseur d'accès, vous risquez de perdre votre compte internet, et si vous causez des dommages réels et qu'elle porte plainte, vous risquez de perdre votre compte en banque. Bref, faire une petite blague à quelqu'un que vous connaissez, c'est une chose, mais ne faites pas ça dans le but de nuire.

QUICKFYRE

http://littlehack.free.fr/download/mailbomb/quickfyre.zip

QuickFyre est un autre mailbomber on ne peut plus simple. L'adresse email de la victime est à rentrer dans "Target", et votre serveur SMTP dans "Server". Il ne reste plus qu'à choisir le nombre d'emails et à cliquer sur "Mail". Avantage par rapport à Saddamme : vous pouvez mieux suivre le déroulement des opérations.



SADDAMME

http://tenkateam2.free.fr/pub/saddamme.zip

Saddamme est un mailbomber très simple d'emploi. Vous remplissez les champs, avec en particulier le serveur SMTP de votre fournisseur d'accès dans "Mail server", et le nombre d'emails à envoyer, et vous cliquez sur "OK Let's Start" en bas à gauche. L'inconvénient du programme : il annonce parfois le succès de l'opération alors que ça n'a pas fonctionné.

ATOMICMAIL

http://amailsender.com/d/ams.exe

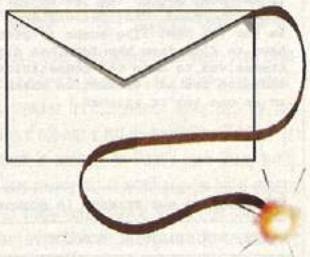
En testant les deux programmes ci-dessus, vous rencontrerez peut-être un problème : certains serveurs mails vous déconnectent après l'envoi d'un seul message, ce qui empêche Saddamme et QuickFyre d'envoyer plus d'un mail (pas terrible pour du mailbombing). Le logiciel Atomic Mail, plus perfectionné (mais payant dans sa version complète, vous ne pourrez envoyer que 50 mails à la fois avec la démo) est prévu plus pour le spam que pour le mailbombing, mais nous allons détourner son usage. Au lancement, tapez votre message, puis appuyez sur F5. Ouvrez le bloc-notes, tapez-y l'adresse de votre cible, puis par copier / coller faites-en une liste conséquente, copiez cette liste et cliquez sur l'icône "Paste from Clipboard" de Atomic Mail.

Voilà, votre liste de destinataires est prête, cliquez sur "OK" puis "Accept". Il ne reste plus qu'à appuyer sur F9 et cliquer sur "Start" pour envoyer du pâté !

Notez que vous pouvez configurer plus de choses en appuyant sur F3. Une autre option intéressante consiste à utiliser le serveur SMTP de votre fournisseur au lieu d'envoyer les mails par le programme (ce qui ne fonctionne pas si votre fournisseur bloque le port 25). Pour cela, allez dans les options ("Settings" / "Common Settings"), et dans l'onglet "ISP's SMTP" remplissez les champs comme suit (en indiquant votre serveur SMTP bien sûr) :

ÇA MARCHE PÔ !!

Tout ça peut ne pas marcher, pour plein de raisons. Pensez à utiliser une adresse email d'origine raisonnable (du genre nimportequoi@hotmail.com), car certains serveurs SMTP vérifient qu'elle est plausible. D'autre part, comme je l'ai déjà dit, certains serveurs refusent d'envoyer trop de mails (ils peuvent aussi limiter le nombre de mails envoyés chaque jour), et de plus en plus de fournisseurs bloquent le port 25 (ce qui pose problème avec Atomic Mail).



Songez enfin que vous n'êtes absolument pas anonymes avec ces programmes, donc allez-y mollo si vous tenez à votre accès internet ! On vous aura prévenu....

GNU/LINUX OU WINDOWS ?

LE RAPPORT QUI VOUS AIDERA À FAIRE VOTRE CHOIX

En tant qu'hackers novices ou informaticiens passionnés, le dilemme "travailler sous Linux ou Windows ?" s'est certainement déjà posé, ou bien se posera très certainement dans les mois à venir en résultat du déploiement de plus en plus marqué de Linux dans l'univers micro. Dans ce numéro nous allons nous pencher sur les atouts qui pèsent en faveur de chacun de ces systèmes d'exploitation, sans entrer dans des campagnes de dénigrement inutiles. Ce comparatif devrait ainsi vous laisser entrevoir plus clairement quel système est adapté à vos besoins.

Nous parlerons dans ces pages de " Linux " comme de GNU/Linux sous ses différentes distributions. Le terme " Linux " désigne, à notre sens, le mode de fonctionnement global d'un système d'exploitation, et nous ne ferons allusion aux différentes distributions de celui-ci (Debian, Slackware, Mandrake, RedHat, Suse, etc. jusqu'à l'infini...) qu'à titre démonstratif. Cet OS est présenté dans l'opinion populaire comme une alternative opposée à Windows, mais voyez-le plutôt comme "différent" de Windows : la qualité globale de ces deux systèmes est, selon l'angle dont on souhaite les considérer, de très bonne facture, bien que la donne ait pu être différente il y a moins de 5 ans.

Nous n'allons pas nourrir les débats partisans qui font la joie des trolls sur IRC : contentons-nous de vous aider à fixer un choix qui s'opérera lorsque vous en sentirez le besoin. Le plus difficile est certainement de trouver des critères de comparaison révélateurs des atouts de l'un et de l'autre : la sélection des critères détermine fortement les conclusions d'une telle démarche. Ainsi un joueur passionné, qui aime se défoncer à l'adrénaline sur des jeux aux graphismes époustouflants, n'aura pas de choix à faire entre Linux et Windows. A ce jour, Windows, grâce au support de DirectX et à la gestion de pilotes matériels performants écrits spécifiquement pour lui, s'avère comme le terrain de pratique dédié aux aficionados du jeu. Même si la tendance se renverse très très légèrement (des supports OpenGL pour Linux existent déjà, ou alors des jeux, tel Unreal Tournament 2003, sont portés sur le système libre), Windows reste LE dominant en la matière. Ainsi pour rendre compte de la problématique, il nous faudrait plutôt par exemple nous intéresser à...

LA SÉCURITÉ :

Windows, à partir de la version 95 jusqu'à la version 2000, a une réputation souillée par les diverses critiques émanant des milieux oeuvrant pour l'(in)sécurité. Windows 95, et 98 sous toutes ses formes, ou encore les serveurs web de Microsoft (tel IIS, jusqu'aux plus récents) sont réputés pour être de vrais "gruyères". A contrario les versions plus récentes du système d'exploitation - 2000, XP, 2003, sous leurs différentes saveurs - sont très nettement marquées par des efforts de Microsoft en la matière. Cette évolution devrait d'ailleurs être de plus en plus prononcée pour les années à venir : les parts de marché de Microsoft se réduisant face à Linux, la volonté de Microsoft est de redorer son blason, de dissoudre les sombres taches qui ternissent son image.

Que ce soit en local ou à distance, la sécurité de ses derniers systèmes Windows est plus aboutie, même si différents bugs logiciels laissent la vie belle aux pirates (pour Outlook, IE, MSSQL, UPnP...). Une machine Windows NT (terminologie qui regroupe Windows NT, 2000/2003, et XP pour les ignares) bien configurée, régulièrement patchée, et faisant tourner le minimum de services est (presque) sécurisée.

Linux ne peut se targuer d'avoir un niveau de sécurité fondamentalement meilleur que celui de Windows. En fait, pour les pirates qui connaissent aussi bien Windows que Linux, l'acquisition de machines sous Linux est bien plus facile : pour peu que la gestion des droits d'accès aux fichiers soit mal effectuée, ou qu'un service soit mal configuré ou non mis à jour, c'est l'intégralité du système qui peut tomber aux mains des hackers. Anecdote révélatrice : la base de données Securityfocus renvoie 263 avis de vulnérabilités sur une recherche avec le mot clef " Windows ", et 251 pour le mot clef " Linux "...

De plus l'activité logicielle d'une machine Linux est moins facilement auditable, ce qui est compensé par le fait que des processus de filtrage, de log, etc. peuvent-être rendus bien plus efficaces que sous Windows.

La sécurité sous Linux est l'aboutissement de méthodes rigoureuses. Une attention particulière doit être accordée à la gestion et au maintien du niveau de sécurité. Sous Windows la sécurité du système repose globalement plus sur la confiance que vous avez dans les applications qui y tournent couramment : allez-vous utiliser un serveur IIS ou Apache ? Lequel rendra votre machine la moins vulnérable ?

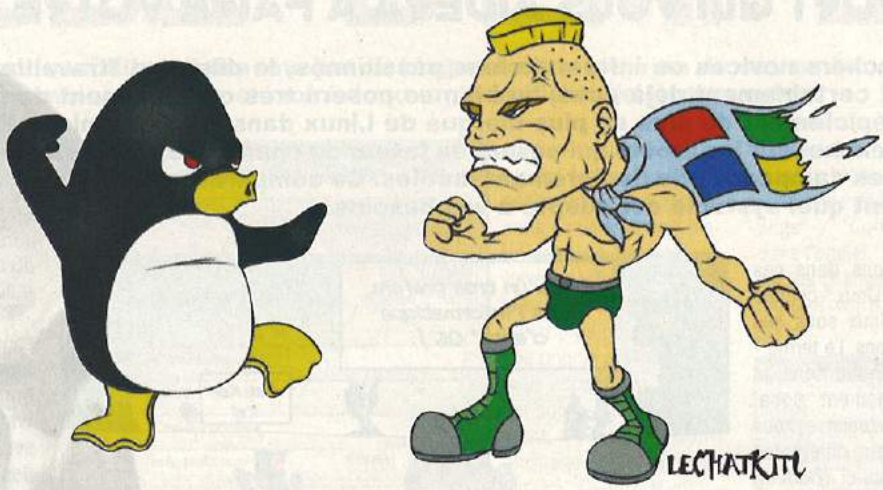
Si vous êtes simple utilisateur, sans la prétention de vouloir transformer votre poste de travail en station serveur, vous pourriez choisir Windows : dénué de Netbios, du service d'affichage de messages, des services de mise à jour sur UPnP, votre station Windows deviendra une véritable forteresse imprenable, un firewall ne servant alors plus à rien. En effet, sans application serveur active, sans service daubique (partage de fichiers avec le c$ par défaut), les points d'entrée sont nuls. A moins que des bugs non découverts soient exploitables au niveau de la pile TCP/IP... (et si vous ne savez pas de quoi il retourne, rassurez-vous, les milliers d'autres lamers qui jouent avec des scanners Netbios ne le savent pas non plus...).

LA STABILITÉ :

Avoir une machine sécurisée est une bonne chose, mais si celle-ci est régulièrement hors service, vous ne serez pas plus avancé. Windows a une réputation d'instabilité très tenace, et ce surtout depuis les versions 95 et 98. A partir de Windows 2000, les utilisateurs apprécieront les améliorations développées pour assurer la stabilité du système. Linux est réputé plus stable que Windows, ce qui est globalement vrai : le kernel Linux, indépendant des applications qu'il lance, est éprouvé maintes et maintes fois par la communauté Open Source. Avant de sortir en version "stable" les noyaux Linux sont dépouillés de tous les bugs découverts pouvant entacher leur stabilité. Autant d'efforts sont-ils réalisés à la relecture du code du noyau Windows ?

En cas de pépin, que ce soit sous Linux ou sous Windows, vous aurez peut-être plus de chances de vous en sortir sous Windows, où les dysfonctionnements sont souvent liés à des applications ou des composants logiciels défectueux, alors qu'il n'y a rien de pire pour un utili-

KINUX PINGUI VS CAP'TAINE WIN



'IZ

LA FÊTE DES AMÉRICAINS...

LE 4 JUILLET

ET CELLE DES HACKERS LE 6

Un concours de piratage a été organisé le 6, plus précisément un concours de défaçage: il s'agissait de modifier la page principale d'un maximum de sites. Ce concours risquait de perturber le trafic sur le net, avait prédit un cabinet de sécurité informatique. Les points étaient attribués selon le nombre de sites qui avaient été défacés. Des points de bonus étaient remis si l'on arrivait à cracker un site fonctionnant avec des logiciels et du matériel informatique de plus haute sécurité (vous vous en doutez, Windows ne valait pas grand-chose en points). Le premier prix devait aller au pirate ou au groupe de pirates qui obtenait le plus de points sur un maximum de 6000 sites en 6 heures. Il y a plusieurs concours de ce genre mais celui-ci a suscité beaucoup plus d'intérêt médiatique. Finalement, beaucoup de bruit pour rien puisque seuls quelques centaines de sites au total ont été piratés, (quelques petits sites mal protégés). Il faut dire que le concours a été un peu ralenti lorsque le site web qui y était dédié a été la cible d'une attaque DoS ;-)

NOUVELLE PROTECTION SUR LES DVD

Même si ses détails ne sont pas très clairs, il existe maintenant une nouvelle protection contre le copiage de DVD. En effet, avec la réédition de Terminator 2 il sera impossible (*hmm*) de copier ce film. Basé sur la nouvelle technologie de Media Player 9 on doit s'enregistrer sur internet avec numéro de série et IP: on ne pourra donc visionner le film sur PC que pour une courte période et il faudra réactiver ses droits pour le revoir par la suite. Un beau succès en perspective pour une technologie si pratique d'utilisation!

sateur Linux qu'un "Kernel Panic" laissant pressentir la réinstallation imminente du système. Et de même, si Linux rencontre des périodes d'instabilité inexpliquées, il n'est pas dit que vous puissiez trouver facilement une solution pratique : des heures peuvent être nécessaires à la simple localisation d'un mystique problème qui n'apparaît que sporadiquement !

Globalement Linux est plus stable que Windows, car lorsqu'il tourne une fois sans problème, il peut tourner dix fois sans problème, et, s'il n'est pas trop sollicité, pour des jours et des semaines... Windows est bien plus stable aujourd'hui qu'il y a quatre ans, mais les problèmes de stabilité restent parfois inexpliqués sous Windows, et il n'est pas rare que l'on doive redémarrer de force la machine qui "rame tellement qu'on ne peut plus faire CTRL+ALT+DEL"...

Quant à l'aspect multitâche de Linux, c'est un vrai plaisir pour la stabilité du système. Il n'y a pas d'explorer.exe qui plante, entraînant la fermeture complète de la moitié des fenêtres en cours de traitement ! Par contre si c'est votre serveur X (le support graphique le plus utilisé pour Linux) qui s'écrase, il ne vous restera plus qu'à choisir entre la corde ou le pistolet.

LA COMPATIBILITÉ MATÉRIELLE :

Un " point chaud " de Linux (pour ne pas dire que certains considèrent cela comme une tare), est sa compatibilité globale avec les matériels récents ou les marques de constructeurs alternatifs aux solutions des géants industriels. Comment votre modem 56k de marque noname va-t-il marcher alors que ces idiots de constructeurs ne vous ont fourni que les drivers pour Windows ?

Actuellement ce sont parfois des particuliers qui assurent bénévolement le développement de drivers pour certains périphériques matériels. Mais heureusement les groupes industriels prennent de plus en plus conscience qu'il y a des efforts à faire à ce niveau. Raison pour laquelle Nvidia, par exemple, assure le développement de drivers génériques pour Linux.

Vous ne devriez pas avoir de problèmes majeurs avec l'exploitation de vos périphériques matériels à l'heure actuelle. Aucun problème en tout cas pour utiliser un disque dur, un lecteur disquette ou CD-Rom et ce quelle que soit leur marque. En effet les montages de tels périphériques au niveau de l'OS ne tiennent que rarement compte des spécifications constructeur avec du matériel standard. D'autres périphériques (carte son, modem, carte réseau...) seront utilisables sous réserve que vous ayez les drivers spécifiques. Vous l'aurez compris : mettre à jour sa configuration matérielle implique de prendre des renseignements sur les supports logiciels qui sont fournis avec les composants que vous désirez acheter.

L'UTILISATION :

L'utilisation de Windows est universellement reconnue comme étant simpliste, ce qui justifie d'ailleurs son succès. On reproche à Linux d'être plus compliqué, trop mystique - le comble pour un système ouvert. Il y a un peu de vrai et de faux dans ces concepts généralistes.

Windows implique une utilisation quasi-exclusive de l'interface graphique, et l'on n'en vient que très rarement à utiliser un système en ligne de commandes tel MS-DOS (ou ce qui s'en rapproche le plus depuis la version 2000) pour effectuer les opérations d'administration. Mais, sous cette allure simpliste qui privilégie la souris au clavier, se cachent des piliers tortueux du système : la base de registres, les répertoires System et System32, etc. Ces parcelles de l'OS sont des fourre-tout sur lesquels l'utilisateur commun ne peut que vaguement trouver de documentation ; "Et cette dll-là elle sert à quoi ?"

Sous Linux, tout est sous forme de fichiers. Le système apparaît ainsi comme une construction de Lego, sauf qu'en lieu et place de briques de plastique, vous avez des fichiers. La configuration de l'immense majorité des applications passe par des fichiers éditables avec un éditeur de texte. L'utilisation de scripts (bash, perl, python...) pour l'installation de logiciels est également monnaie courante. C'est pourquoi l'on a tendance a considérer que Linux est un système pour développeur avant tout.

Et ce n'est pas faux. En fait on peut nuancer ce point de vue : disons que des notions de programmation aident fortement à aller plus loin à la mise en place d'applications logicielles hautement flexibles. L'apprentissage de l'utilisation de base d'un compilateur tel GCC est, par exemple, très fortement conseillé.

Néanmoins les utilisateurs apprécieront la diversité du choix des distributions qui rendent les difficultés de prise en main variables. Une distribution Mandrake est plus simple à installer, à configurer, et à exploiter qu'une Slackware. Mais même si le système est rendu plus accessible aux débutants, un apprentissage sera nécessaire à tout utilisateur désirant exploiter profondément les fonctionnalités de l'OS. La gestion des erreurs, l'utilisation des différentes applications passent nécessairement sous Linux par la lecture des pages de manuels (RTFM !), et un certain niveau d'anglais est souvent requis. Tenez-vous-le pour dit : Linux n'est pas un système pour paresseux du bulbe rachidien.

Peut-on faire la même chose sous Linux que sous Windows ? Cette question hante peut-être votre esprit. Nous avons expliqué que Windows était plus performant pour les applications vidéoludiques que Linux. Windows a un avantage supplémentaire, qui est inhérent à son statut quasi-monopolistique sur le marché des ordinateurs individuels : le vaste panel de logiciels commerciaux qui lui sont dédiés, dont certains sont de très bonne qualité. Les professionnels ayant besoin d'un système d'exploitation pour des tâches telles l'écriture de texte, la composition de morceaux de musique, de pages web, etc. n'ont pas intérêt à miser sur une exploitation de Linux s'ils ne trouvent pas d'équivalents à leurs applications courantes. Les raisons sont multiples : il faut notamment que les fichiers produits soient compatibles avec les applications des autres membres d'une équipe de travail pour ne pas paralyser le circuit productif. Par ailleurs il paraît parfois peu évident de trouver des équivalents à des logiciels commerciaux ayant déjà plusieurs années d'expérience dans certains domaines (comme pour la création d'œuvres numériques).

Pour toute utilisation courante du système (lecture de mp3, de DivX, téléchargement d'œuvres libres de droits sur eMule ou eDonkey...) Linux est absolument opérationnel. Soulignons un avantage que possède Linux du fait qu'il ne soit pas aussi populaire que Windows : il est bien moins polluable que ce dernier. Il n'existe pas d'équivalent Linux (ouf !) à l'armée de Spywares qui sont glissés dans les applications Windows mises en ligne, comme vos codecs Divx.... Les risques de contamination par virus sont également plus faibles – radicalement plus faibles, et ce non pas parce que le déploiement d'un virus sous Linux est impossible, mais parce que les méthodes d'infection seraient tellement spécifiques à ce système qu'en fin de compte les virus ne s'étendraient pas très loin.

LA COHABITATION :

Certains de ceux qui lisent cet article actuellement n'ignorent sans doute pas qu'il est possible de faire cohabiter Linux et Windows sur un même ordinateur. Ce choix implique d'effectuer un certain travail sur le système : il faut segmenter les places où s'installent les différents systèmes d'exploitation. Autant vous pouvez installer simultanément Windows 98, 2000, XP sur une même partition FAT32, autant vous ne pourrez jamais installer votre i386-Linux Debian Sarge testing next 3.1 prerelease sur une partition FAT32 (encore moins NTFS...) où loge déjà un autre Windows. Cette segmentation s'obtient en partitionnant un disque dur, ou en utilisant plusieurs disques durs.

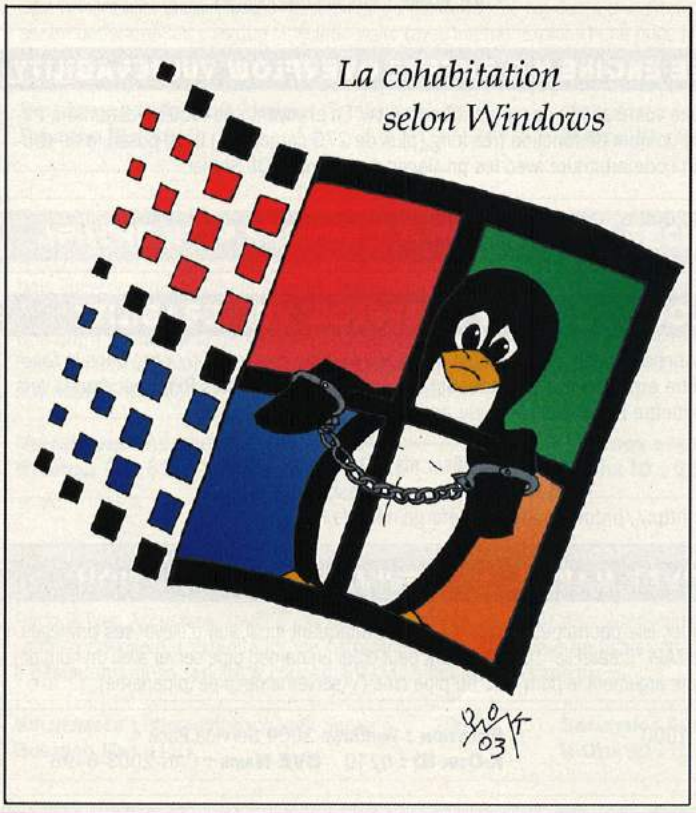
Windows, par choix de la part de son éditeur, n'intègre pas de gestion native des systèmes de fichiers alternatifs à FAT ou NTFS. Exit donc la possibilité de lire vos fichiers Linux sur ext2fs, alors que lire les partitions FAT32 ou NTFS depuis Linux s'avère possible. Linux ne s'arrête pas à garantir la compatibilité avec les systèmes de fichiers Windows, il rend également possible la compatibilité de dizaines de systèmes de fichiers différents, issus du monde Unix ou d'OS morts.

Au niveau applicatif la dualité du démarrage sur différents OS est gérée par des logiciels qui s'inscrivent dans le secteur de boot (Master boot record), avec un outil comme Grub. Mais si l'installation de Linux permet de réécrire facilement la MBR pour restaurer des options de démarrage multi-OS, une réinstallation de Windows écrasera totalement la MBR, monopolisant la zone d'amorçage. Pensez donc à faire une disquette de boot pour votre Linux !

D'autres logiciels pour Windows comme VMWare ou Explore2fs permettent respectivement de démarrer virtuellement Linux ou de visiter les systèmes de fichiers Linux. Il apparaît que la philosophie d'utilisation de Windows implique de subir des restrictions natives sur l'opérabilité de l'OS, tandis que c'est plutôt la dynamique contraire qui prime sous Linux : le degré d'ouverture pour la maîtrise absolue du système Linux est bien plus grand que celui de Windows.

Globalement la cohabitation présente plus d'avantages que d'inconvénients. Même en travaillant exclusivement sous Linux il reste déconseillé de se priver complètement d'un système Windows à portée de main. Mais comme toute fonctionnalité, la gestion du démarrage de multiples OS peut présenter certains inconvénients. Une réécriture manquée de la MBR, des modifications de priorité des périphériques au niveau du matériel de stockage, et vos systèmes pourraient bien devenir impossibles à démarrer.

Globalement si vous penchez pour un système dans le désir de le dominer (root is god allmighty !), une solution Linux se profilerait plus pour vous. Si Linux vous fait peur, des distributions telles Mandrake ou RedHat peuvent servir de passerelle pour une transition " en douceur ". Et si vous êtes un traditionaliste, que vous préférez un système qui pense majoritairement plus pour vous que vous ne pensez à lui, Windows restera votre cheval de course pour un petit temps encore... le temps que de nouveaux efforts d'investissement de la part des éditeurs de logiciels professionnels rendent les solutions Linux plus attractives encore pour ceux qui ont besoin d'un environnement de travail ou de jeu plus performant.



THE VOCODER

BLIZZARD ENTERTAINMENT: RIEN NE VA PLUS?

L'entreprise qui a conçu Warcraft et Diablo s'enfonce dans les sables mouvants puisque ses fondateurs ont démissionné (avec rien de moins que l'ami Bill Roper). Blizzard avait été acheté par Vivendi Universal, et on parle de nouveau d'autant plus de revente que ses fondateurs ne sont plus en poste. Toutes ces démissions coïncident avec certaines rumeurs selon lesquelles Vivendi Universal se débarrasserait de Vivendi Universal Games. Toutefois, les projets comme Warcarft en ligne n'ont pas été annulés. Alors les amateurs, ne désespérez pas!

CISCO DIT, CISCO FAIT

Une nouvelle vulnérabilité a été publiée juste trop tard pour l'inclure dans notre liste de ce numéro. Elle affecte les routeurs Cisco, c'est-à-dire la grande majorité des routeurs gérant le trafic internet. Cette vulnérabilité est de type déni de service: il est possible de bloquer les routeurs à distance, ce qui a à peu près le même effet qu'une grève de péage sur l'autoroute un week-end de départ en vacances. La fin juillet a donc été déclarée semaine noire par Bison Futé. En effet, l'exploit correspondant à la faille a été divulgué dès le lendemain, ce qui a fait craindre des attaques en masse de la part des gentils hackers souhaitant rappeler aux ingénieurs système qu'ils devaient patcher au plus vite. Aux premières nouvelles, seuls quelques cas isolés de tentatives de DoS ont été reportés, sans réussite majeure pour les hackers. "Nous pensons que les hackers se sont mis au travail dès qu'ils en ont entendu parler" a déclaré un spécialiste de la sécurité. Heureusement donc que les hackers se lèvent en général plus tard que les ingénieurs système.

LES VULNERABI

Nous entamons dans ce numéro une nouvelle rubrique en collaboration avec l'Equipe Technique de www.K-OTik.com. Vous y trouverez toutes les principales vulnérabilités apparues en juin-juillet, et pourrez ainsi suivre ce qui se passe dans ce domaine très actif de la sécurité informatique. Mais avant la revue proprement dite, un petit lexique basique s'impose...

BUGTRAQ ID : SecurityFocus (Bugtraq) est une base de données américaine où sont classées toutes les failles de sécurité (ID, Description, Solution ...)
http://www.securityfocus.com

K-OTIK ID : K-OTik est une base de données française où sont classées toutes les failles de sécurité (ID, Description, Solution ...)
http://www.k-otik.com

CVE : (Common Vulnerabilities and Exposures) est une base de données internationale où sont répertoriés les noms des failles de sécurité.
http://www.cve.mitre.org

CROSS SITE SCRIPTING : Vulnérabilité qui touche certains sites Web dynamiques (Moteurs de recherche, forums, url...), et qui permet par exemple l'exécution de code javascript (coté client) ou encore le vol de cookies.

BUFFER OVERFLOW / OVERRUN : Vulnérabilité permettant le crash d'une application en écrivant dans une zone mémoire temporaire plus de données qu'elle ne peut en contenir, ce qui permet par la suite l'exécution d'un code arbitraire.

DENIAL OF SERVICE (DoS) : Le Déni de Service provoque un consommation abusive de la mémoire ou de la bande passante, ce qui provoque le blocage du système, sans qu'il n'y ait d'intrusion.

DIRECTORY TRAVERSAL : Vulnérabilité permettant l'accès à des répertoires système au delà du répertoire autorisé (comme le répertoire web d'un site internet), en général grâce à des caractères "../.."

NETSCAPE 7.02 CLIENT DETECTION TOOL PLUG-IN BUFFER OVERRUN

Netscape souffre d'une vulnérabilité de type buffer overrun. Ce problème se situe dans un plugin qui manipule des application/x-cdt Mime type. Un attaquant peut exploiter ce problème en envoyant un email à la victime contenant un fichier attaché, le code arbitraire sera exécuté avec les privilèges de l'utilisateur qui double cliquera sur ce lien.

VULNÉRABLE : Netscape 7.02 for Windows
K-OTIK ID : 0246
SOLUTION : Effacer le plugin CDT (npcdt.dll)
CVE NAME : Pas encore assigné

MICROSOFT JET DATABASE ENGINE 4.0 BUFFER OVERFLOW VULNERABILITY

Microsoft JET database engine souffre d'une vulnérabilité de type buffer overflow. En envoyant une requête distante à travers JET 4.0 OLE DB Provider, et contenant un nom de fonction très long (plus de 276 caractères) il est possible de causer un buffer overflow, et donc exécuter un code arbitraire avec les privilèges du compte SQL Server.

VULNÉRABLE : Microsoft SQL Server 7 & 2000
K-OTIK ID : 0245
SOLUTION : Microsoft Jet 4.0 Service Pack 7
CVE NAME : Pas encore assigné

LINUX NFS-UTILS "XLOG[]" BUFFER OVERFLOW VULNERABILITY

Une vulnérabilité de type buffer overflow touche nfs-utils, ce problème est causé par une erreur (off-by-one) dans la fonction "xlog()". Cette vulnérabilité pourrait être exploitée par un attaquant en envoyant des requêtes RPC spécifiques vers le service rpc.mountd, ce qui pourrait permettre l'exécution de code arbitraire.

VULNÉRABLE : nfs-utils version 1.0.3
K-OTIK ID : 0244
SOLUTION : Utiliser nfs-utils version 1.0.4
CVE NAME : Pas encore assigné
URL : http://prdownloads.sourceforge.net/nfs/

MICROSOFT SQL SERVER NAMED PIPE PRIVILEGE ESCALATION

Une vulnérabilité touche Microsoft SQL Server, elle pourrait être exploitée par un attaquant local afin d'élever ses privilèges. Cette vulnérabilité est due à une erreur dans l'API "CreateFile" : Un attaquant peut créer un named pipe server avec un nom arbitraire, puis exécuter xp_fileexist avec comme argument le nom UNC du pipe créé (\\servername\pipe\pipename).

VULNÉRABLE : Microsoft SQL Server 7 & 2000
BUGTRAQ ID : 8128
SOLUTION : Windows 2000 Service Pack 4
K-OTIK ID : 0240 **CVE NAME :** CAN-2003-0496

'IZ

LES HACKERS AURAIENT LE CONTRÔLE D'AU MOINS 3 MILLIONS DE SITES

Selon des recherches (plus ou moins) scientifiques, Trustcorps déclare que le pirate moyen contrôle 600 systèmes. En effet, il estime qu'il y aurait environ 1000 groupes de pirates détenant au moins 12 000 systèmes, chacun durant une période de 6 mois. Le but de ces pirates serait d'avoir le contrôle de ces sites, rien de plus (ou presque). Toujours selon Trustcorps, les pirates attaquent habituellement des systèmes qu'ils peuvent pénétrer facilement, ce qui explique ces chiffres élevés. Vous n'avez que 3 ordis sous votre contrôle? Au boulot!

MICROSOFT TENTE DE BOUFFER GOOGLE

Microsoft tente maintenant de monopoliser le domaine des moteurs de recherche sur internet, et plus particulièrement de concurrencer le géant Google. En effet, Microsoft a lancé un nouveau moteur de recherche, MSNBot, qui offre ses résultats sous forme d'index de liens et de documents HTML. Le développement de MSNBot sera échelonné sur plusieurs années et il sera conçu afin de faire le pont entre les particuliers et les entreprises. De plus, les responsables du projet espèrent que le moteur de recherche pourra s'intégrer aux sites web, aux logiciels et au système d'exploitation. La recherche se ferait à partir du portail MSN jusqu'à un nouveau système de fichiers qui sera conçu pour la nouvelle version de Windows (tant mieux, suis-je le seul à avoir de sérieux soucis pour chercher une chaîne dans un fichier sous XP?). En tout cas, tout ça ressemble bien à la même stratégie adoptée par MicroSoft dans le domaine des browsers internet: forcer un maximum de monde à utiliser leur produit afin d'en faire le numéro 1 "par défaut". Tiens bon, Google!

LITES DE L'ETE

MACROMEDIA COLDFUSION MX / JRUN SOURCE CODE DISCLOSURE

Une vulnérabilité a été identifiée dans Macromedia ColdFusion MX et JRun qui pourrait être exploitée par un attaquant distant afin d'avoir accès à des informations sensibles. Il est possible d'afficher le code source des pages ".cfm", ".cfc", ".cfml", ou ".jsp" grâce à un simple "espace" (%20) ajouté à la fin de l'extension du fichier.

VULNÉRABLE : ColdFusion MX JRun 4.0
SOLUTION : ColdFusion MX Updater 3 / JRun 4.0 Updater 2
K-OTIK ID : 0239
CVE NAME : Pas encore assigné

WINDOWS 2000 UTILITY MANAGER PRIVILEGE ESCALATION [MS03-025]

Une vulnérabilité a été identifiée dans Windows 2000, elle pourrait être exploitée par un utilisateur local afin d'augmenter ses privilèges. Ce problème résulte d'une erreur de validation et de manipulation des messages Windows par le Gestionnaire d'Utilitaires (utilman.exe), ce qui pourrait être exploité en envoyant un message Windows spécifique au Gestionnaire d'Utilitaires, permettant ainsi l'exécution de code arbitraire avec les privilèges "Local System".

VULNÉRABLE : Microsoft Windows 2000
SOLUTION : Patch MS03-025
BUGTRAQ ID : 8154
K-OTIK ID : 0238 **CVE NAME :** CAN-2003-0350

MICROSOFT WINDOWS SMB BUFFER OVERFLOW VULNERABILITY [MS03-024]

Une vulnérabilité de type buffer overflow, pouvant causer un Déni de Service, a été identifiée dans Windows SMB. Cette faille résulte d'une erreur dans la validation des paramètres liés aux paquets SMB. Un attaquant (authentifié par le service SMB) peut causer un buffer overflow en envoyant un paquet SMB spécifique contenant un paramètre Taille trop petit.

VULNÉRABLE : Microsoft Windows NT - 2000 - XP
SOLUTION : Patch MS03-024
BUGTRAQ ID : 8152
K-OTIK ID : 0237 **CVE NAME :** CAN-2003-0345

MICROSOFT WINDOWS HTML CONVERTER BUFFER OVERFLOW [MS03-023]

Une vulnérabilité touche toutes les versions de Windows, elle est due à une erreur dans "html32.cnv". Un attaquant peut causer un buffer overflow dès que la victime visite (avec Internet Explorer) une page HTML contenant un code spécifique. L'exploitation réussie pourrait permettre l'exécution de code arbitraire avec les privilèges de l'utilisateur qui consulte cette page HTML.

VULNÉRABLE : Microsoft Windows (Toutes Versions)
SOLUTION : Patch MS03-023
BUGTRAQ ID : 8016
K-OTIK ID : 0236 **CVE NAME :** CAN-2003-0469

APACHE HTTP SERVER 2.0.46 MULTIPLE SECURITY VULNERABILITIES

Trois vulnérabilités touchent Apache Server : La première est liée à SSLCipherSuite, la seconde touche le prefork MPM (Multi-Processing Modules). La dernière faille quant à elle est liée à FTP proxy et IPv6.
Une autre vulnérabilité de type Déni de Service existe dans Apache HTTP Server, elle pourrait être exploitée par des utilisateurs locaux afin de causer un DoS sur une machine vulnérable. Ce problème est lié au gestionnaire type-map (utilisé pour la négociation des ressources et contenus).

VULNÉRABLE : Apache HTTP Server 2.0.46
SOLUTION : Apache version 2.0.47
BUGTRAQ ID : 8134
K-OTIK ID : 0235 **CVE NAME :** CAN-2003-0192

MICROSOFT OUTLOOK WEB ACCESS HTML ATTACHMENT SCRIPT EXECUTION

Outlook Web Access est touché par une vulnérabilité de type Cross Site Scripting, qui pourrait permettre l'exécution de scripts coté client. L'exploitation de ce problème se fait grâce à un fichier attaché HTML, elle pourrait permettre l'accès à des informations sensibles concernant l'utilisateur ou le domaine.

VULNÉRABLE : Microsoft Exchange Server 5.5 - 2000
SOLUTION : Aucun patch officiel pour l'instant.
BUGTRAQ ID : 8113
K-OTIK ID : 0233 **CVE NAME :** Pas encore assigné

UNE VICTOIRE POUR LES CONSOMMATEURS

EMI France a été condamné à verser une somme de 10 000 euros en dommages et intérêts à une association ayant porté plainte à cause de l'écoute d'un disque trop compliquée. En effet, des mesures avaient été prises pour qu'on ne puisse copier ce CD, ce qui va à l'encontre du code de la consommation qui autorise à faire une copie de sauvegarde pour usage personnel. Cette plainte a été déposée par l'union fédérale des consommateurs contre EMI France et Warner afin que cette procédure n'entre pas en conflit avec le code de consommation.

LE VIRUS DES SPAMMERS

Selon certains experts, plusieurs spammers envoient des virus qui transforment les ordinateurs des internautes en véritables poubelles. Un cabinet de filtrage de spams en Angleterre a ainsi identifié le premier virus envoyé par des spammers. Environ un demi-million d'exemplaires du virus AVF ont été envoyés à des internautes sur une période de deux jours le mois dernier. Le virus AVF n'est pas comme les autres virus qui envoient des virus à tous les contacts d'un utilisateur. Celui-ci installe une backdoor par laquelle les spammers peuvent vous envoyer des spams. En plus d'utiliser le PC pour envoyer des spams de sexe ou bien des régimes miracles (sans compter les dernières techniques d'allongement du pénis), il peut le faire anonymement puisqu'il est impossible de retracer son origine. Les internautes savent qu'ils doivent maintenir leur système antivirus à jour pour ne pas se retrouver dans une position inconfortable. Les spammers ont toujours été une nuisance, maintenant ils emploient carrément des méthodes complètement illégales!

CCBill whereami.cgi arbitrary command execution vulnerability

Une vulnérabilité existe dans le fichier whereami.cgi de CCBill, elle pourrait être exploitée afin d'exécuter des commandes à distance sur un système vulnérable. Il est possible d'exécuter des commandes avec les privilèges du serveur web, à travers le paramètre "g" de whereami.cgi.
ccbill/whereami.cgi?g=cat%20../../../../etc/password

Vulnérable : CCBill E-Commerce
Solution : Aucun patch officiel pour l'instant.
Bugtraq ID : 8095
K-Otik ID : 0229
CVE Name : Pas encore assigné

Windows 2000 ShellExecute API buffer overflow vulnerability

Une vulnérabilité de type buffer overflow touche la fonction "ShellExecute()" utilisée afin d'exécuter une application associée à une extension spécifique. Cette faille peut être exploitée en envoyant au paramètre "lpszFile" un argument de plus de 4000 bytes. Le problème a été identifié dans la version 5.0.3502.6144 de "shell32.dll" (d'autres versions pourraient être vulnérables).

Vulnérable : Microsoft Windows 2000
Solution : Windows 2000 Service Pack 4.
Bugtraq ID : 8090
K-Otik ID : 0228
CVE Name : Pas encore assigné

Microsoft Commerce Server insecure registry permissions

Une vulnérabilité à été identifiée dans Microsoft Commerce Server, qui pourrait permettre à un attaquant local d'avoir accès à des informations sensibles. Le mot de passe est enregistré dans la clé registre "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Commerce Server", ce dernier est codé mais accessible pour n'importe quel utilisateur.

Vulnérable : Microsoft Commerce Server 2002
Solution : Changer les permissions Registre: HLM\SOFTWARE\Microsoft\Commerce Server
Bugtraq ID : 8063
K-Otik ID : 0227
CVE Name : Pas encore assigné

Windows 2000 Server Active Directory buffer overflow vulnerability

Une vulnérabilité de type buffer overflow a été identifiée dans Active Directory. Cette faille peut être exploitée en envoyant une requête de recherche LDAP v3 contenant 1000 opérateurs "AND" ou "OR", ce qui provoquera le crash de "Lsass.exe" puis le reboot du système.

Vulnérable : Microsoft Windows 2000 Server
Solution : Windows 2000 Service Pack 4
Bugtraq ID : 7930
K-Otik ID : 0225
CVE Name : Pas encore assigné

Windows NetMeeting Directory Traversal Vulnérabikity

Windows NetMeeting est un outil de visioconférence (audio/vidéo). Une vulnérabilité de type Directory Traversal touche l'option "File Transfer".
Un attaquant peut exploiter ce problème en transférant un fichier contenant des caractères "..\..\" et l'uploader dans n'importe quelle partie du disque de la victime (au delà du répertoire de réception par défaut - ex : C:\Program Files\NetMeeting\fichiers reçus).
L'attaquant peut donc exécuter des commandes arbitraires en transférant par exemple un fichier DLL spécifique qui remplacera un existant dans le répertoire NetMeeting, et sera exécuté dés le redémarrage du programme.

Vulnérable : NetMeeting version 3.01 (4.4.3385)
Solution : Windows 2000 SP4 - Windows XP SP1
Bugtraq ID : 7931
K-Otik ID : 0224

Adobe Acrobat Reader Unix buffer overflow vulnerability

Acrobat Reader souffre d'une vulnérabilité de type buffer overflow, qui pourrait être exploitée par un attaquant distant afin d'exécuter un code arbitraire en incitant l'utilisateur à cliquer sur un lien malicieux. Cette faille se situe dans la fonction WWWLaunchNetscape qui utilise un buffer de 256 bytes pour stocker un lien.

Vulnérable : Adobe Acrobat Reader Unix v5.0.7
Solution : Utiliser Adobe Acrobat Reader 6.0
Bugtraq ID : 8069
K-Otik ID : 0219

Chaouki BEKRAR aka ReYn0 (Consultant Sécurité - A.D.Consulting)

Les musiciens contre la RIAA

Bien qu'ils perdent eux aussi de l'argent à cause du P2P, les musiciens se portent à la défense d'étudiants poursuivis en justice par la RIAA. En effet, les musiciens prétendent que ce n'est pas en envoyant les fans en prison ou en les réduisant à la faillite personnelle qu'ils achèteront les albums par la suite. Bien qu'ils défendent les droits d'auteur et qu'ils aient de la reconnaissance pour le travail des artistes (c'est-à-dire le leur), ils ne désirent en rien que les fans se désintéressent de la musique. Toujours selon eux, tous ces procès contre le P2P n'aident pas au développement d'une technologie pour protéger les droits d'auteur tout en ayant accès à la musique de notre choix sur Internet. C'est pourquoi les musiciens indépendants se portent à la défense des étudiants qui ont été inculpés pour avoir partagé de la musique sur le web, au vu des sommes exorbitantes réclamées par la RIAA. Ils ont lancé une pétition dénonçant les méthodes de la RIAA. Allez, un petit script et ils devraient bien recueillir un bon million de signatures...

Apple position

Le service de musique en ligne d'Apple, iTune, connaît un véritable succès. En effet, dès la première semaine l'entreprise a vendu plus d'un million de chansons. Selon un des dirigeants d'Apple, la vente des chansons accessibles sur Internet surpasse tout espoir et changera à jamais la façon d'acheter de la musique. Il affirme que les gens sont prêts à payer pour obtenir les chansons de leur choix. Il s'agirait peut-être d'une nouvelle manière de produire et de consommer légalement de la musique sur Internet, selon le président de Warner Music.

MICROSOFT WINDOWS MEDIA SERVICES REMOTE SYSTEM ACCESS

Microsoft Windows Media Services est touché par une vulnérabilité de type buffer overflow. Cette vulnérabilité ne touche que les systèmes Windows 2000 avec Internet Information Services IIS 5.0. Ce buffer overflow est lié à l'extension ISAPI (Internet Services Application Programming Interface) nsiislog.dll, son exploitation pourrait permettre l'exécution de code arbitraire avec les privilèges du serveur IIS.

Vulnérable : Microsoft Windows Media Services 4.1 - IIS 5.0
Bugtraq ID : 8035
Solution : Patch MS03-022
K-Otik ID : 0208
CVE Name : CAN-2003-0349

MICROSOFT WINDOWS MEDIA PLAYER ACTIVEX MEDIA LIBRARY ACCESS

Un contrôleur ActiveX inclus avec Windows Media Player 9 Series est touché par une vulnérabilité, qui pourrait permettre à un attaquant distant d'avoir accès à la librairie media de l'utilisateur. Afin d'exploiter ce problème l'attaquant devra obliger la victime à visiter ou à cliquer sur un lien web contenant du code html malicieux.

Vulnérable : Windows Media Player 9 Series
Bugtraq ID : 8034
Solution : Patch MS03-021
K-Otik ID : 0207
CVE Name : CAN-2003-0348

SYMANTEC SECURITY CHECK ACTIVEX REMOTE BUFFER OVERFLOW

Symantec offre un service de scan online (Symantec Security Check), afin d'exécuter ce scan l'utilisateur devra accepter l'installation de composants ActiveX. Ces composants ActiveX nommés "Symantec RuFSI Utility Class" ou "Symantec RuFSI Registry Information Class" sont vulnérables à un buffer overflow qui résulte de la combinaison d'un long argument avec la fonction CompareVersionStrings.
Cette faille pourrait permettre à n'importe quel site web d'activer l'un des deux contrôleurs ActiveX installés sur la machine de l'utilisateur, et donc utiliser la fonction CompareVersionStrings afin d'exécuter du code arbitraire.

Vulnérable : Symantec Online Security Check
Bugtraq ID : 8008
Solution : Effacer "Symantec RuFSI Utility Class"
K-Otik ID : 0196

PROFTPD MOD_SQL SQL INJECTION VULNERABILITY

ProFTPD combiné à mod_sql souffre d'une vulnérabilité de type SQL Injection. Elle peut être exploitée par un attaquant distant afin d'avoir accès au ftp sans authentification.

Vulnérable : ProFTPD version 1.2.9rc1
Bugtraq ID : 7974
Solution : Ne pas utiliser mod_sql avec ProFTPD
K-Otik ID : 0192

INTERNET EXPLORER CUSTOM HTTP ERROR SCRIPT INJECTION

Une faille de type Script Injection touche Internet Explorer, cette vulnérabilité est liée aux pages d'erreurs générées par IE. Lorsqu'un site web affiche une erreur 404, Internet explorer inclut l'url du site dans la page d'erreur res://shdoclc.dll/404_HTTP.htm#http://site.com/file.html, cette procédure d'inclusion est touchée par une faille qui pourrait permettre l'exécution de code arbitraire.

Vulnérable : Microsoft Internet Explorer 5.0 - 5.5 - 6.0
Bugtraq ID : 7939
Solution : Désactiver Active Scripting
K-Otik ID : 0184

INTERNET EXPLORER XML FILE CROSS-SITE SCRIPTING

Une faille de type CSS touche Internet Explorer, ce problème résulte d'une erreur dans la manipulation de certains fichiers XML. Si Internet explorer rencontre une erreur, il affiche l'url du fichier xml, ce qui pourrait permettre l'exécution de commande en insérant des scripts dans ces liens.
Afin d'exploiter la vulnérabilité, un attaquant doit trouver un serveur avec un fichier xml qui ne peut pas être affiché correctement par IE, l'attaquant devra ensuite pousser la victime à cliquer sur un lien.

Vulnérable : Microsoft Internet Explorer 5.5 - 6.0
Bugtraq ID : 7938
Solution : Aucun patch n'est disponible.
K-Otik ID : 0183

PHP SESSION ID CROSS SITE SCRIPTING VULNERABILITY

Une vulnérabilité qui touche PHP vient d'être publiée : elle permettrait à un utilisateur distant de conduire des attaques de type Cross site Scripting. Cette faille résulte d'une erreur dans la variable "PHPSESSID" qui ne vérifie pas les caractères avant de les valider. La faille est exploitable seulement si l'option "transparent SID support" est activée.

Vulnérable : PHP 4.3.x - 4.2.x - 4.1.x - 4.0.x
Bugtraq ID : 7761
Solution : Utiliser PHP version 4.3.2
K-Otik ID : 0150
CVE Name : CAN-2003-0442

BIG "FBI" BROTHER

Un projet de loi a été déposé au Congrès américain qui ferait en sorte que le FBI enquêterait sur la violation des droits d'auteur et poursuivrait les utilisateurs. Le FBI développerait des techniques visant à dissuader ceux-ci de télécharger du matériel protégé par les droits d'auteur. En plus, de nouveaux agents formés en piratage et en droit sur la propriété intellectuelle travailleraient sur ce projet. Selon eux, cela effraiera les gens de penser que le gouvernement les surveille. Quelle blague, on n'a plus peur depuis Loft Story!

SURPROTECTION

L'utilisation d'une nouvelle technologie de protection des droits d'auteur sur les CD a créé une fois de plus la controverse. En effet, un jeu PC distribué en Australie a donné bien des maux de tête aux détaillants et aux utilisateurs. Atari Corp. (ex-Infogrammes) a lancé l'extension du sublime Neverwinter Nights. Cette extension se vend très bien chez les détaillants: 9000 exemplaires écoulés en Australie. Toutefois, ce n'est que rendus à la maison que les clients se sont aperçus que le jeu gelait leur ordinateur ou qu'il ne fonctionnait pas avec leur lecteur de CD/DVD-ROM. De même, un détaillant de Berlin a reçu plusieurs plaintes et tous les employés de ce magasin ont testé le jeu sur leur propre PC: dans la majorité des cas, l'extension ne fonctionnait tout simplement pas. Atari a déclaré qu'il n'était pas question de retirer le produit du marché et que l'extension, à cause du système de protection, avait seulement quelques problèmes de compatibilité avec certains lecteurs CD/DVD-ROM. La solution? Télécharger NEVERWINTER.NIGHTS.SHADOWS.OEUNDRENTIDE-DEViANCE.

DEFACAGES EN MASSE

Ça fait pas mal d'outils que vous regardez, de beaux articles que vous lisez ;-)) mais là, devant votre PC, ce soir, vous ne savez vraiment pas quoi faire... Ok, elle est belle cette liste de raccourcis vers des beaux toolz sur votre bureau, mais il vous faut de l'action, de la vraie, comme au cinéma ! Héhé, je vois que déjà, ces deux phrases vous ont bien fait baver, alors on va enchaîner les amis.

Etape une, s'essuyer la bouche. Etape deux, libérer les amis. Etape trois, regarder du côté de zone-h.org. La page de garde donne entre autres des informations comme celles-là :

ZONE-H IN NUMBERS

2 legal advisors
18 operators
6 super operators
5 admins
9 super admins
2795 mail subscribers
212193 digital attacks
3421 forum messages
3521 downloadable files
6528 attacks on hold
205 users on-line

Ça montre que ya du monde qui bosse ce jour-là.... non ?` ;-))

Je n'ai pas besoin d'attirer votre attention sur le chiffre en rouge, hein ! Ensuite, en approfondissant un peu plus la lecture, du côté des OS (juste en dessous), on va avoir la surprise du chef, le plus hacké des OS c'est ? .... c'est ..... Krosoft ?

ZONE-H TODAYS REPORTED ATTACKS

131 single IP
1847 mass defacements

Linux (92.1)
Win 2000 (6.7)
Unknown (0.3)
Win NT9x (0.3)
SolarisSunOS (0.3)
FreeBSD (0.2)
IRIX (0.2)
... (0.1)

Et non !!!!!

Et dans le genre écart entre le peloton et le leader en tête, le Pingouin se débrouille pas si mal :)) Les présentations sont maintenant faites, il reste à voir plus en détail ce qui se passe, s'est passé, et bien sûr ce qui va/risque de se passer dans les jours/minutes qui viennent sur le net.

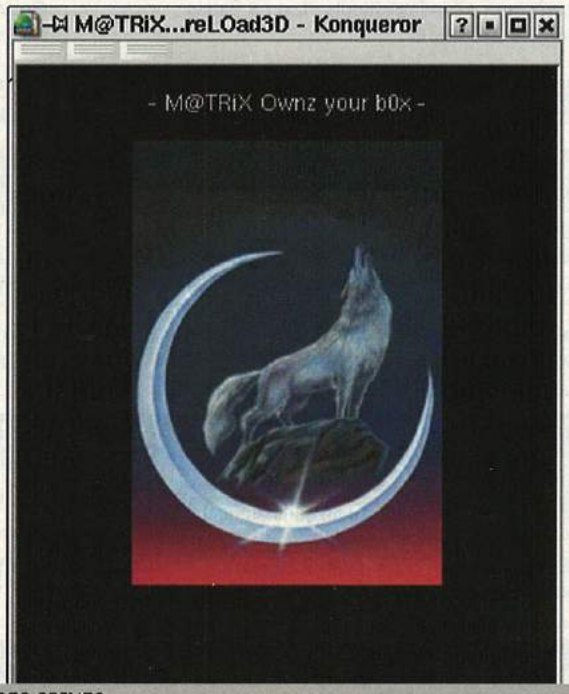
Alors, de mon plus beau clic gauche je vais me diriger vers les "Attacks archives" (menu de gauche). Ok, ok me diront les puristes (et j'en vois pas mal en train de lire ces lignes d'ailleurs :)) , ce sont des jeuneZ qui font du deface, et le deface c'est pas beau....

Mais bon, le but ce n'est pas de faire la même chose, mais de regarder et d'apprendre.

Et là, après le clic gauche magique, me voilà sur une page recensant tous les derniers sites défigurés.

Il y en a des mieux, mais je ne vais pas tout vous montrer quand même, hein !! En fouillant un peu, vous pourrez admirer les plus belles pages défacées, et apprécier le sens esthétique et la créativité de ces vilains pirates.

Ceci étant dit, après cette période de contemplation béate, vous pouvez aller visiter des rubriques plus intéressantes comme les news, mais là, je pense que vous avez tous les moyens de trouver l'information comme des grands que vous êtes :))



SITE PIRATES/ARCHIVES DES CRIMES

[Activer les filtres |]

Aujourd'hui , les sites pirates: 2295 dont 172 sont des piratages d'IP individuels et 2123 sont des piratages en masses

Legende:
H - Piratage de site persos
M - Piratage en masse (Cliquez pour voir tout les sites pirates de cette IP.)
R - Re-piratage (Cliquez pour voir tout les antecedents de ce site.)
★ - Piratage special

Horaire	Hacker		Domaine	OS	Voir
00:39	Uberlamers	M	...-haut.de/wwwboard.html	Linux	infos | mirroir
00:39	Uberlamers	M	...artei.de/wwwboard.html	Linux	infos | mirroir

DETAILS SUR CE PIRATAGE

Horaire/time:	2003/07/20 00:[illegible]9
Hacker:	Uberlamers
Domaine:	http://[illegible]/wwwboard.html
Mirroir:	./defaced/2003/07/18/[illegible]/wwwboard.html/
Adresse IP:	18[illegible]2
Systeme:	Linux
Serveur:	145
Methode d'attaque:	
Information extra:	piratage en masse

Dans le genre il y a de quoi faire ... c'est pas mal hein (2295 sites en cours de piratage), et lorsque je veux en savoir plus, il suffit d'un petit clic pour obtenir un résumé de l'action archivée :

LES FAILLES D'UNE BOUTIQUE EN LIGNE

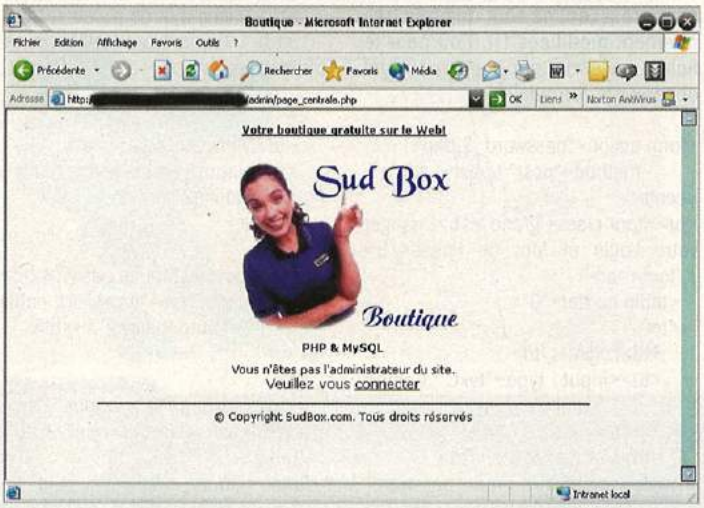
En consultant ma boîte mail, comme à l'habitude, un mail attira particulièrement mon attention. On me demandait simplement si je pouvais aller faire un tour sur une boutique avant son ouverture histoire de voir si je ne pouvais pas trouver une petite faille... C'est la première fois qu'on me demande un " pseudo audit ", je commence donc avec joie mon investigation...

ADMIN

Le premier dir à consulter, le dossier admin ! Allons y faire un petit tour...

Je tombe sur une page d'administration tout à fait classique avec Login et Mot de passe.

A tout hasard, je rentre " admin " et " password " et arrive bien entendu sur : " Vous n'êtes pas l'administrateur du site, blablabla " :



Nous pouvons remarquer le copyright SudBox. Après une courte recherche, je retrouve et télécharge le script de boutique utilisé ici : " Pas de connaissances en programmation pour réaliser votre boutique sur le Web. Avec SudBox Boutique, vous allez rapidement créer votre propre boutique de commerce électronique. Le script comprend en mode administration différents modules : création et gestion de la boutique (configuration complète en mode admin. Mot de passe, login, devises, tva....) Mise en page des fiches produits avec: Prix, TVA, frais de port, photos, gestion des articles épuisés....) Gestion des commandes en ligne..). Installation rapide (création automatique des tables dans votre base de données MySQL.) "

Ce qui est sympa, c'est que le site est alors en " OpenSource " ; nous allons donc pouvoir tester plein de bidouilles en local... ce que nous n'aurions pas pu nous permettre sur le serveur.

Ainsi après un petit tour dans les pages du dossier admin, nous pouvons voir que les pages sont protégées par une session des plus classiques :

```
<?
session_start();

if (!session_is_registered('login')) {
   header("Location:page_centrale.php");
}
?>
```

La lecture de la page n'est possible que si la session 'login' est enregistrée. D'où un premier bug : l'exploitation de la page [même sans pouvoir lire la page, nous avons accès aux noms des variables utilisées, grâce au script].

Autre souci, sûrement dû à un manque d'attention du concepteur de la boutique, l'oubli (?!) du script de session dans quelques pages.

Voici les fichiers pour lesquels ces lignes manquent avec ce que cela nous permet sans être loggué :

A) AJOUTER_CAT.PHP
En allant sur http://[boutik]/admin/ajouter_cat.php, nous tombons sur une page nous demandant le nom de la rubrique à ajouter ! Plutôt sympa comme petite attention.

B) AJOUTER_SOUSCAT.PHP
Idem, hormis le fait que l'on peut insérer une photo pour illustrer la sous-rubrique, le tout sans restriction de taille... de quoi faire un joli petit "deface".

C) CENTRE_HAUT.PHP
Complètement inutile mais nous y avons accès... :)

D) INDEX.PHP (*)
Nous verrons toutes les possibilités que nous offre cette page plus loin.

E) LOGIN.PHP
Idem !

F) MENU.PHP
Accès à des infos diverses : nombre d'articles, de sous-catégories et catégories ainsi que le nombre de commandes activées.

G) MENU2.PHP
Sûrement la page la plus importante de l'admin... elle nous donne la date !

H) MENU_GAUCHE.PHP
Nous affiche le menu d'administration.

I) PAGE_CENTRALE.PHP (*)
C'est la page de refoulage (vue plus haut), que l'on obtient lorsqu'un mauvais mot de passe a été entré ou lorsque l'on essaie d'accéder à une page protégée par le code vu plus haut.

J) PAGE_PRINCIPALE.PHP
Dans cette page, une erreur de code nous donne le path du site. Nous pouvons aussi créer nous-mêmes une erreur pour faire afficher ce path. Cette faille, appelée 'Path Disclosure', nous indique le répertoire dans lequel le site se situe dans le serveur.

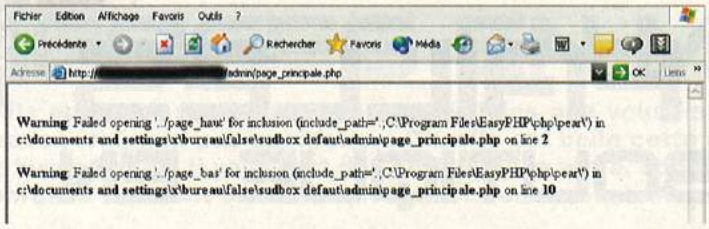
K) PASSWORD.PHP

NOTRE PAUVRE DISQUETTE

La commission Brun-Buisson, après avoir tout taxé, s'acharne sur la pauvre disquette. Pourquoi? Parce qu'il s'agit selon eux d'un moyen redoutable de piratage!!! Nous devrons dorénavant payer 1,5 centimes d'euros de plus afin d'enrichir de plus belle la Sacem and co..Ils ne désirent pourtant pas taxer encore plus les CD vierges, mais plutôt concevoir un système anti-copie sur les CD audio. Toutefois, quel est l'intérêt de taxer une disquette de 1.44 Mo sur laquelle il est impossible de mettre un mp3 en entier, sans parler d'un jeu?

LES JEUX GAMECUBE ENFIN PIRATÉS

On attend toujours le premier modchip pour GameCube. Mais pendant qu'on attend, les groupes pirates eux ont décidé qu'ils en avaient marre, et ont sorti sur le net les images CD des jeux de la dernière console de Nintendo. Vous trouverez par exemple les fichiers .nfo correspondant dans la nouvelle section GameCube de www.nforce.nl. Si vous cherchez bien, vous arriverez peut-être même à télécharger les jeux (pas sur NFOrce par contre, inutile de perdre votre temps à chercher). Par contre, n'espérez pas y jouer pour l'instant. Même s'il y a eu plusieurs annonces de modchips, elles se sont toutes révélées être des canulars jusqu'à présent. Gardez quand même un oeil sur www.gcdemos.com, qui annonce un modchip pour très bientôt promis juré c'est vrai mais ma maman me l'a confisqué il faut attendre encore un peu. En attendant, vous pourrez peut-être vous consoler en espérant que le dernier émulateur GameCube annoncé soit un vrai cette fois-ci. Des captures d'écran ont été publiées sur le site www.emulation64.com... Vivement plus d'infos!



Cette page nous permet de changer le login et mot de passe de l'admin sans avoir les anciens !
Regardez plutôt :

L) QUITTER.PHP (*)

Cette page nous permettra de nous de logguer quand nous serons parvenus à rentrer dans l'admin ;)

M) TOP.PHP

Cette page nous est complètement inutile, elle sert à faire joli dans l'admin !

Ici, sans aucun effort ni même de connaissances particulières, comme vous pouvez le constater, nous avons un nombre incroyable de possibilités, dont le changement du mot de passe de l'admin !

A mon humble avis, il devrait y avoir pas mal de travail sur ce site... mais ne nous arrêtons pas en si bon chemin.

PREMIÈRE PHASE DE SÉCURISATION.

Pour commencer, nous allons protéger en lecture toutes ces pages oubliées en remplaçant au début de chacune d'elles (sauf celles indiquées par une astérisque (*)) les lignes :

```
<?
include("../page_haut.inc");
?>
```

Par :

```
<?
session_start();

if (!session_is_registered('login')) {
  header("Location: page_centrale.php");
}

include "../page_haut.inc";

?>
```

Nous n'autorisons donc la lecture que si la session 'login' est enregistrée, comme vu plus haut.

C'EST REPARTI !

A) ATTAQUE DE PASSSWORD.PHP

Comme je l'ai bien précisé, nous venons d'empêcher seulement la lecture des pages et non l'exploitation ! Nous pouvons donc encore exploiter certaines de ces pages. Le site étant en OpenSource, nous connaissons le nom des variables par défaut (qui ne sont que très très rarement modifiées !). D'où pour le fichier password.php, nous pouvons observer le formulaire :

```
<form action="password_2.php"
      method="post" target='_top'>
<center>
<br><font class='grand'><b>Changer
votre Login et Mot de Passe</b>
</font><br>
  <table border="0">
  <tr>
    <td>Login: </td>
    <td><input type="text" name=
        "admin"></td>
  </tr><tr>
    <td>Mot de passe: </td>
    <td><input type="password"
        name= "motdepasse"></td>
  </tr><tr>
    <td colspan="2">
    <input type="submit" value="En-
      voyer"></td>
  </table>
</form>
```

Ainsi pour modifier le mot de passe, il nous suffit de composer :
http://[boutik]/admin/password_2.php?admin=CisKo&motdepasse=PasS

Nous obtiendrons alors en retour la page " Vous n'êtes pas l'administrateur... " mais le code aura bien été interprété ! Le couple login/pass aura donc bien été modifié !

B) SÉCURISATION DE PASSWORD.PHP

Pour pallier à ce problème de sécurité, nous pouvons tout simplement modifier le nom des variables 'login' et 'motdepasse'. La lecture de la page venant d'être empêchée précédemment, il sera alors impossible de reconstituer la requête. Mais comme à Pirat'Z nous ne faisons pas les choses à moitié, nous allons demander les anciens login et pass pour autoriser le changement... au cas où un pirate aurait réussi à s'introduire dans l'admin... ce que nous verrons un peu plus loin.

Pour ce faire, nous allons modifier le formulaire de la page password.php comme ceci :

```
<form action="password_2.php"
      method="post" target='_top'>
<center>
<br><font class='grand'><b>Changer
votre Login et Mot de Passe</b>
</font><br>
  <table border="0">
    <tr>
      <td width="126"> Ancien login:
      </td>
      <td width="175"> <input type=
        "text" name="admin"></td>
    </tr>
    <tr>
      <td>Ancien mot de passe:</td>
      <td> <input type="text" name=
"motdepasse"></td>
    </tr>
    <tr>
      <td>Nouveau Login: </td>
      <td><input type="text" name=
          "admin2"></td>
    </tr>
    <tr>
      <td>Nouveau Mot de passe: </td>
      <td><input type="password" name
          ="motdepasse2"></td>
    </tr>
    <tr>
      <td colspan="2"><input type=
        "submit" value="Envoyer"></td>
  </table>
</form></form>
```

Nous avons ainsi ajouté les champs 'admin' et 'motdepasse' et remplacé les deux autres en 'admin2' et 'motdepasse2', afin de demander l'ancien couple login/pass.

Il nous faut maintenant modifier password_2.php pour vérifier l'ancien login et mot de passe.

Remplacer ceci :

```
$query = mysql_query("SELECT admin,
         motdepasse FROM $sbbadmin");
$num = mysql_num_rows($query);
$update = mysql_query("UPDATE
  $sbbadmin SET admin='$admin',
  motdepasse='$motdepasse' WHERE
  id='1'") || die (mysql_error());
```

Par :

```
$query = mysql_query("SELECT admin,
         motdepasse FROM $sbbad-
         min");
```

'IZ

LES ARTISTES VEULENT PLUS QUE 99 CENTS!!!

Plusieurs artistes ont une certaine réserve quant à émettre leurs singles sur des sites payants à cause des droits d'auteur, et parce que le concept d'album risquerait de devenir chose du passé. Ce processus a des répercussions importantes en bout de ligne: les artistes ne diviseront plus les recettes du CD entre les différentes étapes de production, mais seulement à coup de 99c (le prix d'un single en téléchargement). C'est encore moins rentable pour les auteurs-compositeurs qui normalement reçoivent une plus grande partie des recettes.

EN ÊTES-VOUS?

Est-ce que la RIAA vous poursuivra? Vérifiez par vous-même sur le site ecf.dcd.uscourts.gov. En effet, les partageurs de fichiers peuvent maintenant se rendre sur ce site et savoir si leur nom fait partie des 871 internautes américains identifiés qui devront comparaître pour piratage. Par contre, il faut d'abord s'enregistrer sur le site, et attendre quelques jours avant de voir son compte confirmé, et il faut payer pour y obtenir des documents. En plus, bizarrement, le site est devenu inaccessible le jour où cette nouvelle a été annoncée. Le site TechTV (www.techtv.com) a lui réussi à obtenir une liste de 253 noms (ou plutôt, nicknames KaZaa), ce qui permet déjà de faire une première vérification (pas toujours très utile, par exemple www.k_lite.tk_Kazaa_Lite@Kazaa doit s'appliquer à pas mal de monde). Le site de l'Electronic Frontier Foundation (www.eff.org) compte aussi mettre une liste similaire en ligne très bientôt. Commentaire d'un malheureux élu de cette liste: "je ne savais pas que c'était illégal". Reste à convaincre le jury...

```
unset($check);
while ($row = mysql_fetch_row($query)) {
  if (($row[0] == $admin)
     && ($row[1] == $motdepasse)) {
        $check = "ok";
  }
}
if (IsSet($check)) {
  $num = mysql_num_rows($query);

  $update = mysql_query("UPDATE
     $sbbadmin SET admin=
     '$admin2', motdepasse=
     '$motdepasse2' WHERE id='1'")
     || die (mysql_error());
} else {
  header("Location: page_centrale.php");
}
```

c) Attaque de login.php

Voici le script permettant d'ouvrir la session 'Login' :

```
<?
session_start();
include "../configuration.php";

$query = mysql_query("SELECT admin,
        motdepasse FROM $sbbad-
        min");

while ($row = mysql_fetch_row($query)) {
  if ($row[0] == $admin)
     && ($row[1] == $motdepasse)) {
        $check = "ok";
  }
}

if (IsSet($check)) {
  $login = $admin;
  session_register('login');
  include("nav.php");
  exit;
} else {
  header("Location: page_centrale.php");
}
?>
```

Ainsi que la plupart d'entre vous ont dû le remarquer, le script compare le couple login/pass contenu dans la base de données avec le couple fourni par le biais du formulaire d'index.php. Si le couple correspond, le script définit la valeur 'ok' à la variable $check. La session ne s'ouvrant que si $check==ok.

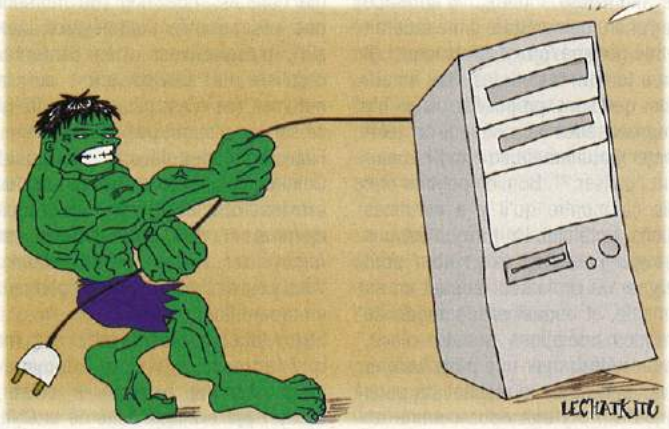
Le problème de ce système est que l'on peut définir nous-mêmes la valeur de la variable ! Ainsi en se rendant à l'adresse: http://[boutik]/admin/login.php?check=ok on accède directement à l'administration !

Pour combler ce trou de sécurité majeur, il suffit de définir la variable check comme nulle à l'aide de la structure unset (thx to Frog-m@n !).

Il faut donc rajouter en début de page :

```
UNSET($CHECK);
```

Pour plus d'informations concernant la structure unset, rendez-vous à l'adresse suivante : http://php3.de/manual/fr/html/function.unset.html



THE END... OUF !

Ca y est, nous en avons enfin terminé avec cette boutique ! Ce petit audit aura été instructif, nous aurons pu voir une multitude de failles et de sécurisation php et nous rendre compte de la vulnérabilité de certains services commerciaux se développant sur le net... Bon, il est justement temps d'aller me commander en ligne quelques produits gratuits ! ;-)

CisKo
. : CisKo@engineer.com : .
Spécial greetz to Frog !

La recherche au service des hackers

Si votre mot de passe Windows est constitué de lettres et de chiffres (comme la plupart des mots de passe), prenez garde! En effet, des chercheurs suisses ont mis au point une méthode pour cracker les mots de passe de Windows en 13,6s (en moyenne). Remarquez, auparavant il ne fallait qu'une minute et 41 secondes en moyenne, ce qui n'est pas énorme non plus. La méthode s'appuie sur un certain nombre de faiblesses de la méthode d'encryption utilisée par Microsoft, en particulier l'absence d'élément aléatoire. Résultat: il est possible de stocker de grosses tables contenant des mots de passe déjà encryptés afin de les comparer ultra-rapidement avec le code à casser. Les 13,6s de moyenne sont obtenues sur un AMD 2500+ avec 1.5 Go de RAM, dans laquelle est stockée une table de 1,4 Go. La solution: utiliser des caractères spéciaux, ce qui augmente la complexité et la taille des tables nécessaires (qui monte à 10-20 Go). Ou désinstaller Windows. En attendant, vous pouvez tester le système en ligne sur http://lasecpc13.epfl.ch/ntcrack/

LES LOIS ANTI-PIRATAGE

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

La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique a créé des infractions spécifiques en la matière, reprises par les articles 323-1 à 323-7 du code pénal. Extraits choisis :

- Accès ou maintien frauduleux dans un système informatique : 1 an d'emprisonnement et 15 000 Euros d'amende.
- Accès ou maintien frauduleux dans un système informatique avec dommages involontaires : modification ou suppression de données, altération du fonctionnement du système 2 ans d'emprisonnement et 30 000 Euros d'amende.
- Entrave volontaire au fonctionnement d'un système informatique : 3 ans d'emprisonnement et 45 000 Euros d'amende.
- Introduction, suppression, modification intentionnelles de données : 3 ans d'emprisonnement et 45 000 Euros d'amende.

EN FRANCE

COMMENT ETRE ANO

L'anonymat sur internet, voilà une vieille utopie à laquelle beaucoup aspirent. Certains pour des motifs peu avouables, d'autres simplement parce qu'ils veulent le respect de leur vie privée. Aujourd'hui, alors que la paranoïa de la traque sur internet grandit, est-il encore possible de rester anonyme sur le réseau ? Telle est la difficile question à laquelle nous allons tenter de répondre au fil de ces pages (là, normalement, la bave vous pend aux lèvres et vous ne pouvez plus vous arrêter de lire).

PEERCACHE POUR CACHER KAZAA

La filiale hollandaise de Wanadoo a déclaré avoir installé "PeerCache", un système de cache mis au point par JoltID, les concepteurs de KaZaa, mieux connus sous le nom de FastTrack. Le logiciel est installé sur un serveur local du fournisseur d'accès, ce qui devrait réduire la quantité de bande passante utilisée par KaZaa et augmenter considérablement la vitesse de téléchargement (et aussi prendre une place conséquente sur le disque dur de Mr Wanadoo!). Par exemple, si un client de KaZaa est connecté à partir de Wanadoo, le logiciel vérifiera d'abord si le fichier demandé est dans le PeerCache du serveur. Si oui, le fichier sera téléchargé directement du cache et dans le cas contraire, il sera téléchargé à partir de l'ordinateur d'un autre utilisateur. Habituellement, seuls les transferts directs sont possibles avec les caches classiques. La différence dans le cas qui nous intéresse est que les fichiers les plus demandés sont divisés en petits bouts, et stockés sur les serveurs du FAI. Reste à savoir si tout cela est bien légal...

NAPSTER INNOVE!

Le fondateur de Napster, Shawn Fanning, tente de développer une nouvelle technologie qui permettrait de télécharger de la musique sans enfreindre la loi sur les droits d'auteur. Ce nouveau programme basé sur des condensés numériques fiables identifiera toutes les chansons offertes sur le réseau. Tous les mp3 soumis seront examinés afin de savoir s'ils sont protégés par le droit d'auteur. Si tout est en règle, les chansons seront téléchargeables moyennant quelques frais. Je sais pas vous, mais moi j'ai comme un doute...

Comme le sujet est assez vaste, posons en tout de suite les limites. Comme je suppose qu'en plus d'être parano, vous êtes également aussi fauché que nous sommes radins, on va laisser de côté la plupart des solutions commerciales. Sachez qu'il en existe beaucoup, et vous êtes libre de les essayer et de nous faire part de vos expériences pour qu'on passe votre témoignage dans le mag', et qu'on se remplisse les poches pendant que les vôtres se vident. Dans ce dossier, ce sont donc les solutions gratuites qui vont être privilégiées, même si pour ça il faudra mettre un peu les mains dans le cambouis.

LE WEB

Commençons donc par le sujet le plus classique mais pas forcément le plus facile : comment surfer anonymement sur le web. En plus, ça va nous permettre d'introduire de nombreux concepts utiles dans les autres sections. Donc, si vous ne le savez pas encore, lorsque vous vous promenez sur un site quelconque, de nombreuses informations personnelles peuvent être récupérées par le serveur, puis stockées à votre insu. On parlera des cookies plus tard, mais pour avoir une idée de ce qu'un simple browser peut dévoiler, visitez une adresse comme http://www.elfqrin.com/binfo.shtml ou encore http://privacy.net/analyze/. Vous pouvez également obtenir le même genre d'informations en français sur la fameuse page de la CNIL : http://www.cnil.fr/traces/

Evidemment, la plupart de ces informations ne sont pas vitales, exception faite de votre adresse IP, qui peut vous trahir irrémédiablement lorsque vous visitez le site de votre ami dont vous avez effacé le disque dur la semaine dernière, et qui justement vous demande d'aller sur sa page perso voir ses dernières trouvailles en matière de design HTML. Vous avez également pu être banni d'un forum de discussion pour votre comportement enjoué qui a été mal perçu, et vouloir aller vous excuser gentiment, mais pour cela il vous faut camoufler votre IP véritable. Bref, on peut trouver plein de bonnes raisons pour vouloir cacher son IP, ainsi que plein de mauvaises, mais ça je sais que je n'ai pas besoin de vous en donner.

L'outil de base que nous allons retrouver à plusieurs reprises, c'est le proxy, mot magique qui fait encore peur à certains. La preuve avec cette perle trouvée sur le forum d'anonymat.org, par une personne dont je respecterai l'anonymat, qui répond à la question "comment fait-on pour être anonymisé?" (sic) : "d'après ce que j'ai cru comprendre il me faudrait un truc nommé 'proxy', mais lequel (il y en a tout un tas sur les sites américains qui sont proposés, et je n'y comprends rien !), où peut-on télécharger gratuitement ce proxy, et comment l'utiliser ?". Bon, on peut en rire, mais ça montre qu'il y a certaines notions à clarifier. Un proxy n'est pas un logiciel. Il s'agit d'un nom pour désigner un ordinateur auquel on se connecte, et auquel on demande de faire des opérations à notre place, comme télécharger une page web, et de nous renvoyer le résultat (la page web). Un proxy agit donc comme un intermédiaire entre notre ordinateur et le site, de façon à ce que nous ne soyons jamais connectés directement au site. Notre adresse IP est alors invisible. Fin du tour de magie.

Maintenant, où se trouve ce fameux proxy ? Il en existe en fait des milliers : il s'agit tout simplement de serveurs sur lesquels tourne un logiciel spécial permettant cette fonctionnalité (il existe de nombreux logiciels différents). On peut classer ces serveurs en deux catégories : les proxies "officiels", c'est-à-dire ceux qui sont destinés à cette tâche, et les "officieux", c'est-à-dire ceux qui n'étaient pas prévus pour ça. Les premiers font de la pub et sont souvent payants, ou très lents s'ils sont gratuits. Les derniers sont des ordinateurs mal configurés, souvent des proxies d'entreprises qui ont oublié de mettre des restrictions sur qui a le droit d'utiliser le proxy. Si personne d'autre que vous n'a découvert leur fonction cachée de proxy, ils peuvent être très rapides, si par contre des centaines d'internautes profitent de leur bande passante, ils peuvent ramer (presque) aussi fort que Windows XP avec 64 Mo de RAM. De plus, ils ne restent que rarement disponibles très longtemps, car l'entreprise finit par se rendre compte d'où vient sa facture de 50000$ d'excès de bande passante du mois dernier (les proxies sont aussi très utilisés par les spammeurs, de façon à pouvoir envoyer impunément des tonnes d'emails sans craindre de voir leur IP bannie). On peut se demander s'il est illégal d'utiliser un tel proxy. A ma connaissance, non (du moment que vos activités sont légales bien sûr), puisque vous vous contentez d'utiliser un service offert sur la machine (ce n'est pas votre faute si ce service n'aurait pas dû exister).
Finie la théorie, place à la pratique! Commençons avec le plus simple, les proxies officiels. L'un des plus anciens et des plus connus est Anonymizer (www.anonymizer.com). Vous pouvez l'utiliser très simplement en tapant l'adresse : http://anon.free.anonymizer.com/http://adresse_a_visiter_anonymement. Comme adresse à visiter, essayez par exemple celle de la CNIL donnée plus haut pour vérifier que votre IP est bien cachée (si vous avez un doute sur votre IP, tapez ipconfig en commande DOS pour la trouver). Malheureusement, dans sa version gratuite Anonymizer bloque certains sites, comme Hotmail, ou les sites sécurisés utilisant HTTPs. Ce n'est donc pas une solution satisfaisant à 100%. Un autre service de surf par proxy est "The Cloak" (www.the-cloak.com), mais la version gratuite est également très limitée (elle interdit notamment les commandes POST, c'est-à-dire tout remplissage de formulaire, donc de login sur un site protégé par mot de passe). Finissons les gratuits avec Anonymouse (http://nonymouse.com/anonwww.html), entièrement gratuit mais pas très perfectionné. Il existe encore d'autres proxies payants proposant un accès gratuit limité, mais je n'ai rien trouvé de bien sensationnel.

Si vous voulez être libre de vos mouvements, il faudra donc y mettre un peu du vôtre, et vous trouver un proxy

NYME SUR INTERNET

par vous-mêmes. Rappelons que nous cherchons un proxy pour le web : par tradition, ces proxies écoutent (reçoivent les requêtes) sur le port 8080, mais on en trouve aussi sur les ports 80 et 3128 (voir l'encadré sur les proxies pour plus de détails). Vous pouvez donc utiliser un outil de scan afin de trouver un tel proxy. Pour cela je vous reporte à l'encadré "Comment scanner". Vous pouvez essayer de faire plus simple en utilisant des proxies trouvés par d'autres. Il existe sur le net de nombreuses listes de proxies, mais malheureusement la plupart du temps elles ne sont pas à jour et aucun ne fonctionne. Certains programmes viennent aussi avec des listes de proxies censées être mises à jour, mais j'en ai testés pour vous et le résultat est le plus souvent décevant. Celle de SocksChain (voir l'encadré qui lui est consacré) est la meilleure que j'ai trouvée. Une autre est celle du site MultiProxy, sur http://www2.multiproxy.org/anon_list.htm, sur laquelle je suis parvenu à trouver deux proxies fonctionnels (si si!). Du côté des sites de listes de proxies, allez donc faire un tour par exemple sur : http://www.stayinvisible.com/index.pl/proxy_list et les liens qui en partent, vous trouverez sans doute votre bonheur.

Bon, maintenant que vous avez un proxy à utiliser (par exemple monproxy.com:8080), il faut encore configurer votre navigateur web pour lui indiquer de passer par le proxy au lieu de se connecter directement aux sites. Sous IE, cela se fait (pour une connexion internet par ADSL ou réseau local) en cochant la case "utiliser un serveur proxy..." dans Outils / Options Internet / Connexions / Paramètres réseau (voir capture d'écran). Si vous utilisez un bon vieux modem 56K, dans le même onglet "Connexions" cliquez sur la connexion puis sur "Paramètres" et cochez la case "Utiliser un serveur proxy pour cette connexion".

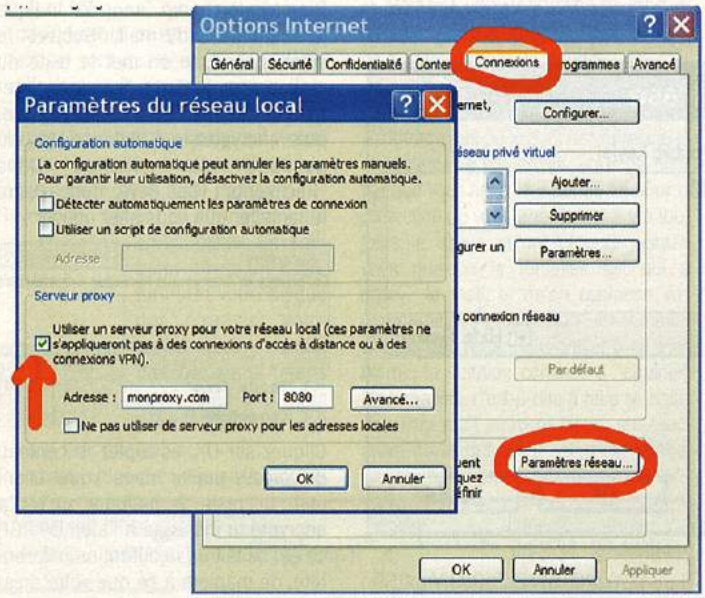
Ensuite, il faut vérifier que le proxy est de type "anonyme", c'est-à-dire qu'il ne révèle pas votre adresse IP au site distant (par exemple en lui disant "au fait, c'est untel qui m'a demandé de récupérer cette page web). Il existe plusieurs méthodes pour vérifier le caractère anonyme d'un proxy, comme le programme MultiProxy, ou à l'aide de sites web, comme http://www.multiproxy.org/env_check.htm : allez à cette adresse après avoir configuré votre navigateur avec votre proxy, et vérifiez que votre véritable adresse IP n'apparaît nulle part sur la page web.

Attention, utiliser un proxy "non officiel" n'est pas forcément exempt de tout danger ! Il faut savoir ce que l'on risque, en particulier :

- ces proxies sont souvent moins perfectionnés que les proxies type Anonymizer.com, ne camouflant pas votre système d'exploitation par exemple, ou d'autres informations système. Les proxies payants offrent aussi souvent des fonctions de blocage des scripts "malveillants" (Javascript et compagnie) pour plus de sécurité.

- des logs sont généralement conservés. Si vous faites une bêtise, votre véritable IP pourra donc être retrouvée par le propriétaire du serveur

- autre problème posé par les logs : vous ne savez pas ce qui est loggué. Quelqu'un d'un peu vicieux pourrait très bien s'amuser à configurer un serveur proxy sur sa machine, attendre que quelqu'un le scanne, et alors espionner les utilisateurs. Je ne vous conseille donc pas de vous connecter à des sites nécessitant des mots de passe que vous devez absolument garder confidentiels, ou de rentrer votre numéro de carte bleue lorsque vous utilisez un tel proxy. Le risque, s'il est minime, n'en vaut pas la peine. D'ailleurs, il est trop tard pour tous ceux qui se sont déjà connectés sur mon proxy test et qui ont consulté leur compte Hotmail ! All your passwords are belong to us.



LE MAIL

L'email anonyme, c'est aujourd'hui la version moderne de la bonne vieille lettre anonyme. Vous savez, celle qu'on écrit en découpant des lettres de journaux, que l'on colle sur du vieux papier, puis que l'on demande à quelqu'un de glisser sous la porte du destinataire... Et bien, c'est presque pareil avec les emails, grâce à des serveurs que l'on appelle...

Les Remailers Anonymes

Un remailer est en gros un serveur à qui on envoie un mail, et qui le redirige vers l'adresse souhaitée. Les remailers dont nous allons parler sont ceux dits "anonymes", c'est-à-dire qui ne dévoilent pas l'origine du message (vous) lorsqu'ils le redirigent. Le destinataire ne peut ainsi pas remonter jusqu'à l'auteur du mail. Intéressé ? Alors, continuez de lire, car si le principe est simple, l'exécution l'est un peu moins, et il y a certaines techniques à maîtriser pour atteindre l'anonymat (presque) parfait.

Tout d'abord, il va falloir installer PGP si vous ne l'avez pas déjà fait. En effet, la plupart des remailers sont configurés pour n'accepter que des messages encryptés pour plus de confidentialité (on y reviendra plus loin). Vous pouvez trouver les adresses où télécharger les dernières versions gratuites de PGP sur http://www.pgpi.org/products/pgp/versions/freeware/.

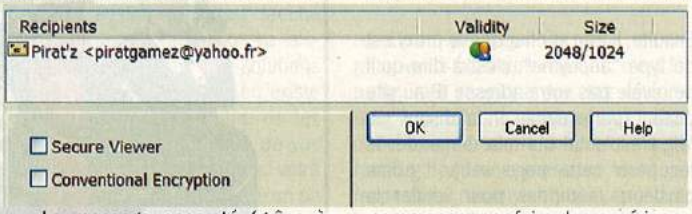
LA RIAA PART EN CHASSE

La RIAA a déjà commencé à intenter des poursuites judiciaires contre certains pirates qui téléchargeaient des mp3. Pour cela, la RIAA a contacté les fournisseurs internet afin d'obtenir l'identité des pirates pour ensuite les poursuivre (seulement les pirates américains... du moins pour l'instant). La RIAA a d'ores et déjà envoyé des citations à comparaître et la cour américaine entend environ 75 causes par jour. Les amendes varient, selon le degré d'infraction, entre 750$ et 150 000$ US. Ça fait beaucoup de numéros de Pirat'z ça...

LA LEN PASSE AU SÉNAT

La LEN, ou " Loi pour la confiance dans l'Economie Numérique " continue tout doucement son petit bonhomme de chemin. Elle est toujours à l'état de projet, mais une nouvelle étape a été franchie avec l'adoption du texte (après modifications) par le Sénat les 24 et 25 juin. Parmi les points les plus importants de ce texte, les hébergeurs pourront être reconnus coupables du contenu illicite qu'ils hébergent s'ils n'ont pas pris les mesures nécessaires pour le retirer lorsqu'on le leur a gentiment demandé. Par contre, les dénonciations abusives visant à faire retirer un site légal sont également punies. Le spam est (presque) interdit, mais encore suffisamment autorisé pour continuer à pulluler dans nos boîtes (vos coordonnées que vous fournissez en ligne pourront être utilisées). La fourniture d'outils de cryptage est réglementée, sous couvert de libéralisation de la cryptologie. La détention de logiciels de sécurité risque de vous rendre hors-la-loi. Le texte est sur : www.telecom.gouv.fr/internet/index_len.htm et la lutte se passe sur www.vie-privee.org.

Lors de l'installation, vous créerez une paire clé publique / clé privée : en résumé, la clé publique est celle que vous donnez à vos amis pour qu'ils encryptent des messages, que vous seul serez capable de décrypter, à l'aide de votre clé privée. Prenons un petit exemple pour être sûr que vous maîtrisiez bien la bête : ouvrez le bloc-notes et tapez un court texte, puis copiez-le par Ctrl-A / Ctrl-C. Cliquez avec le bouton droit sur la petite icône de PGP, et sélectionnez Clipboard / Encrypt. Dans la liste "Recipients", vous devez mettre les destinataires du message, en l'occurrence vous, puisqu'il ne s'agit que d'un test, puis cliquer sur OK.

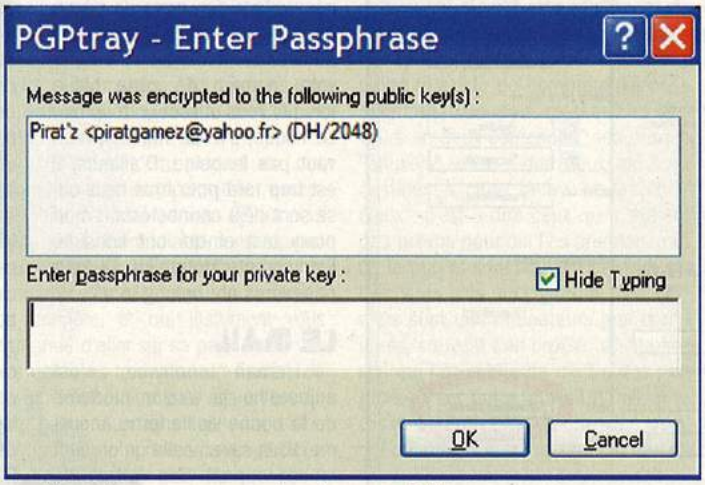


Le message encrypté (grâce à votre clé publique) est alors copié dans le presse-papier, vous pouvez le visualiser dans le bloc-notes, ça doit ressembler à ça :

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

qANQR1DBwU4DA+05PLAbrXIQB/0Q1/bG4mEfiAi4mg/HkOuf8CrgmdGrYPnsB2N3
o19w4j7p9Xx1ODOP100PmDD9LMA+nwVUDuXG/u04wyXgyfnVHo17yaiJNFVAUz/+
Uah+9WRshaL6RwWyD6W0FqrQ3ezynPl60ts00Z4bkLULITq+pl/rLHF0r2z37dwY
-----END PGP MESSAGE-----

Pour le décrypter, un nouveau clic droit sur l'icône de PGP, et cette fois-ci on choisit Clipboard / Decrypt and Verify.



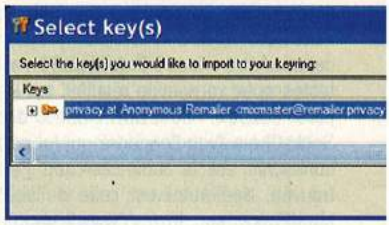
Vous devrez encore rentrer la "passphrase" correspondant à votre clé privée : c'est une phrase qu'on vous a demandée lors de la création de votre paire de clés, et qu'il ne faut jamais oublier sous peine de ne plus pouvoir décrypter ses messages (il est également conseillé de ne jamais l'écrire nulle part, et de ne pas prendre des phrases trop classiques, comme "Pirat'z est le meilleur magazine du monde").

Bien, maintenant nous allons utiliser un remailer pour envoyer un mail crypté anonyme. Le principe est le suivant : vous envoyez le mail crypté au remailer, qui le décrypte et l'envoie en clair au destinataire final. Pour cela, il vous faut bien sûr la clé publique du remailer. Nous allons commencer par faire des expériences avec le remailer "austria" (mixmaster@remailer.privacy.at), mais s'il ne marchait pas au moment où vous lisez cet article, voyez un peu plus loin pour d'autres remailers. Pour demander une clé publique à un remailer, il faut lui envoyer un email dont le sujet contient simplement "remailer-key" (sans les guillemets). La réponse arrive généralement dans la minute qui suit, et contient plusieurs clés, en principe une clé Mixmaster et deux clés PGP, de la forme :

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mixmaster 2.9.0 (OpenPGP module)

mQCNAziXaLgAAAEEAOlgQxgxJ4zdkZeY3db4vHK4qZYCN+wh+A31848WBNC+1/9S
Ca56PnaE/yTA3P5AW5Da4g96KoL-MyPQQwuRPzglX1yCK6NIDqE/7Y3AfZPcpyBd1
ikG8aaWzaNZTBV/EyEn0P3IVrpgTS9oMa5SIDabEDakWv3sj38LCjIDvaPU1AAID
-----END PGP PUBLIC KEY BLOCK-----

Pour l'instant intéressons-nous uniquement aux clés PGP. Les deux clés correspondent aux protocoles RSA (la plus courte) et DH/DSS (la plus longue). Il vous suffit d'une seule, c'est généralement la DH/DSS qui est la plus utilisée, mais vous prendrez pas de très grands risques en utilisant la RSA (pour plus d'informations sur les différences entre les deux protocoles, visitez http://www.scramdisk.clara.net/pgpfaq.html). Copiez donc le bloc correspondant à la clé (en incluant "-----BEGIN PGP PUBLIC KEY BLOCK-----" et "-----END PGP PUBLIC KEY BLOCK-----") , puis cliquez sur l'icône PGP, encore sur Clipboard / Decrypt and Verify.



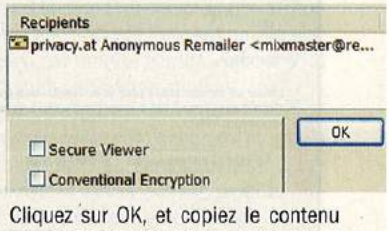
Vous devez voir la clé du remailer, il ne reste plus qu'à cliquer sur "Import" pour pouvoir l'utiliser. Maintenant, allez dans votre client mail (ou dans le bloc-note), et tapez votre email. Cet email doit avoir un format spécial, de la forme :

```
::
Anon-To: Pirat'z <piratgamez@yahoo.fr>

##
Subject: Au secours
```

ARRÊTEZ TOUT DE SUITE VOTRE MAG, CAR LE MIEN NE SE VEND PLUS ! PITIÉ !

Bien sûr, le champ "Anon-To" indique le destinataire du mail, "Subject" le sujet, et ensuite on met le texte du mail proprement dit. Il faut maintenant crypter tout ça : copiez le texte, puis encryptez-le à l'aide de la clé publique du remailer. Dans "Recipients", vous devez donc mettre le remailer que vous allez utiliser :



Cliquez sur OK, et copiez le contenu du presse-papier dans votre client mail. Il reste à indiquer qu'on a encrypté le message à l'aide de PGP, ce qui se fait en rajoutant un petit entête, de manière à ce que votre mes-

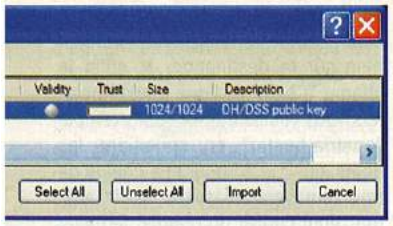
sage final ressemble finalement à :

```
::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

qANQR1DBwE4DTpBM/M97kj4QA/4q
UCcm4FNYbDMmq4fjVu6PEH0PYuCWZ
PVU53Ws
hpqXR+BZSvdaVl7RXb11IpFEdNQt-
SoiWxdjjjwi+fXzx61Ko0r8TQvIRMym-
zHOSO
6ofH9tundoy9pXN3aurR9U9wVv4BpiS
F9djct3835in6U1KIXK9VJQ5ilmAS3UG
V
-----END PGP MESSAGE-----
```

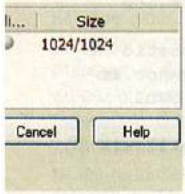
Vous enverrez cet email à **mixmaster@remailer.privacy.at**, sans rien mettre dans le sujet. Il est conseillé



de vérifier d'abord que tout fonctionne bien en s'envoyant un email à soi-même. Attention ! La plupart des remailers ont un certain "temps de latence", c'est-à-dire que votre email ne sera pas envoyé immédiatement à son destinataire. Il y a plusieurs raisons à cela :

- déjà, un remailer peut se retrouver particulièrement chargé, et votre mail devra donc attendre avant d'être pris en compte
- d'autre part, introduire un délai fait partie du processus d'anonymat. Savoir à quelle heure exacte un certain mail a été envoyé peut en effet démasquer la personne qui est derrière.
- pour encore plus de sécurité, les mails ne sont pas envoyés dans l'ordre dans lequel ils sont reçus. Cela permet d'éviter que quelqu'un puisse retracer un email en analysant le trafic (ce n'est pas quelque chose de facile à faire, mais c'est possible).

Soyez donc patient en attendant votre



email, faites un solitaire, buvez un coca, formatez votre disque dur, étranglez votre grand-mère, enfin bref passez le temps tranquillement sans vous stresser. Il devrait finir par arriver.

Pour savoir plus précisément combien de temps on peut s'attendre à attendre (par exemple une vingtaine de minutes pour le remailer austria), il existe des pages web de statistiques, qui sont également une bonne source d'adresses de remailers. Vous en avez par exemple sur : **http://mixmaster.shinn.net/stats/remailer-list.html** et sur **http://anon.efga.org/Remailers/TypeIList**. Regardez dans la liste à la fin, il y a des stats du type :

remailer	email address	history	latency	uptime
austria	mixmaster@remailer.privacy.at	+**********	0:23:34	99.49%

Il est conseillé de choisir un remailer ayant un uptime (pourcentage de temps de fonctionnement) aussi haut que possible, et un temps de latence ("latency") aussi bas que possible (si vous voulez que votre email arrive vite bien sûr, ce qui n'est pas forcément le cas). Vous pouvez également trouver des pages web contenant les clés publiques des remailers, mais il est plus sûr de la demander directement au remailer par la commande remailer-key. D'autres commandes utiles (à mettre dans le sujet d'un mail) sont remailer-conf (pour savoir comment est configuré le serveur), remailer-stats (pour voir des stats sur le nombre d'emails traités), et remailer-help (si vous êtes perdu). La configuration d'un remailer est particulièrement importante. Elle est synthétisée par une ligne du type "cpunk mix pgp pgponly repgp remix latent hash cut test ek ekx esub inflt50 rhop20 reord klen1024". Les options les plus importantes pour ce qui nous a intéressés jusqu'à présent sont "cpunk" (Cypherpunk Remailer, c'est-à-dire acceptant les messages cryptés) et "pgp" (supporte l'encryption par PGP).

Avec tout ça, vous devriez être capables d'envoyer de jolis mails anonymes. Mais si vous êtes vraiment paranos, vous avez peut-être entendu parler de rumeurs selon lesquelles certains remailers seraient maintenus par le FBI, la CIA et même le magazine Pirat'z. Certes, ce ne sont que des rumeurs, mais rien ne dit qu'elles ne sont pas fondées (oui, j'aime entretenir votre paranoïa). Même si les remailers anonymes ne gardent officiellement pas de logs et ne vérifient pas le contenu de vos emails, vous ne pouvez que vous fier à leur bonne foi pour la protection de votre anonymat : il y a toujours le risque qu'on remonte jusqu'à vous puisque le remailer sait qui a envoyé le mail, et qu'on espionne vos communications puisque le remailer peut le décrypter. Pour pallier à ce problème, la solution consiste à "chaîner" les remailers, c'est-à-dire à faire se balader votre mail entre plusieurs remailers avant de le délivrer à son destinataire. Par exemple, supposons que vous vouliez utiliser une chaîne R1 - > R2 - > D, où R1 et R2 sont des remailers et D la destination. Vous commencez par créer un email comme si vous utilisiez juste le remailer R2. Vous rajoutez alors l'en-tête suivant :

```
::
Anon-To: adresse_R2
```

puis vous encryptez cet email pour l'envoyer à R1 (donc avec la clé publique de R1). Lorsque R1 le reçoit, il le décrypte (mais seulement la première "couche" de cryptage) et s'aperçoit qu'il doit l'envoyer à R2. R2, lui, décrypte la seconde couche et l'envoie à D. Intérêt : seul R1 connaît l'origine, et seul R2 connaît le contenu et le destinataire (ça, vous n'y pouvez pas grand chose, puisque le message doit être envoyé en clair au destinataire). Evidemment, vous pouvez introduire d'autres remailers au milieu, qui eux ne connaîtront ni l'origine, ni le destinataire, ni le contenu du mail (d'où l'intérêt de l'encryption systématique). Donc tant pis pour le FBI (et pour nous) : espionner le trafic ne sert plus à rien. Notez que les remailers qui ont le mot-clé "middle" dans leur configuration sont configurés pour automatiquement relayer votre email à au moins un autre remailer avant livraison, si vous n'avez pas spécifié de chaîne vous-mêmes.

Le Maître du Mix

Et ce n'est pas fini ! Certains ont trouvé que l'anonymat n'était pas suffisant avec un tel système, ce qui a donné naissance à un autre type d'encryption pour les remailers, appelé "Mixmaster". Les remailers compatibles avec ce protocole sont appelés remailers de type 2 (alors que les remailers "Cypherpunk" sont de type 1), et sont caractérisés par la présence du mot-clé "mix" dans leur configuration (la plupart des remailers de type 2 sont également compatibles avec le cryptage de type 1). Mixmaster est spécialement conçu pour renforcer la sécurité dans les chaînes de remailers : l'encryption est basée sur RSA et le triple DES, et les messages ont tous la même taille (28.1 Ko) et sont réordonnés, de manière à empêcher de les suivre par l'analyse du trafic. Par contre, l'inconvénient est qu'il faut utiliser un programme spécial pour construire ses mails anonymes. Les deux programmes les plus utilisés sont QuickSilver (**http://quicksilver.skuz.net/**), la dernière version au moment d'écrire cet article se trouve sur **ftp://skuz.net/pub/quicksilver/QS.9b20.11.4.exe**) et Jack B. Nymble 2 (**http://www.bigfoot.com/~potatoware/jbn2/index.html**).

Comme il faut bien faire un choix, c'est QuickSilver que je vais vous

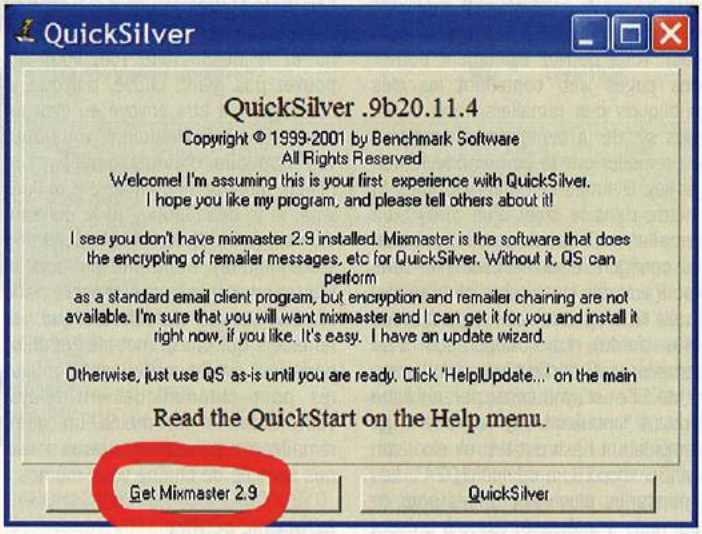
Le P2P en prison

Deux républicains veulent déposer un projet de loi qui enverrait les utilisateurs de P2P directement en prison. Grâce à leur projet, il serait plus facile d'attraper les gens qui téléchargent des mp3, des films, etc. sur un réseau de P2P. En prenant en considération que chaque fichier émis a été téléchargé au moins 10 fois, selon leur calcul cela représenterait une valeur au détail de 2500$, ce qui en ferait un acte criminel grave et l'accusé se verrait peut-être infligé d'une peine de 5 ans de prison. À quand la guillotine?

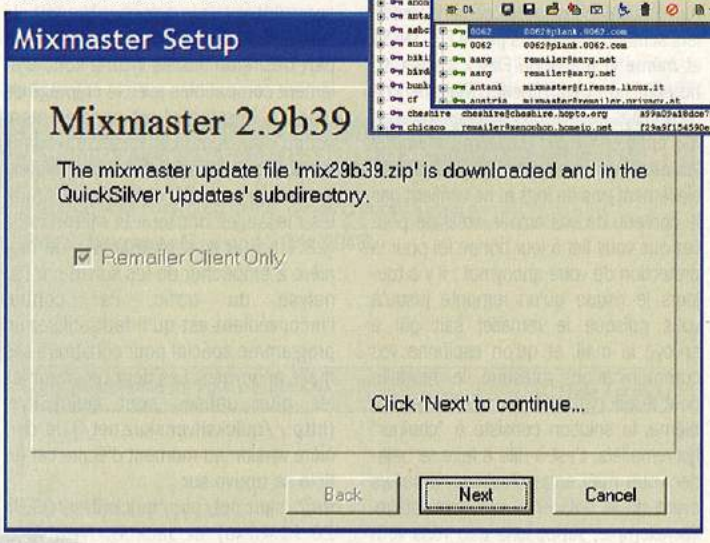
Le courriel jetable contre le pourriel

Quand vous souhaitez vous inscrire sur un site web où l'on vous demande une adresse de messagerie valide afin de vous faire parvenir votre nom d'utilisateur et votre mot de passe, vous craignez de donner votre véritable adresse de peur d'être envahi par les spams (après le courriel du Québec, voici le pourriel...je sais ils sont bizarres!). Eh bien, il existe maintenant un nouveau site internet où l'on vous offre des adresses courriels jetables. En effet, le site jetable.org offre des adresses pour une durée limitée, de 24 heures à 8 jours. Il s'agit d'un service de redirection de mail. Il faut donc entrer votre véritable mail et la durée pour laquelle vous aurez besoin de l'adresse jetable...tous les mails seront par la suite transférés directement dans votre vrai compte. Vous n'avez qu'à répondre au formulaire du site jetable.org, et ensuite on vous attribuera votre nouvelle adresse. Il s'agit d'un excellent moyen de préserver l'anonymat et de ne pas se faire envahir par les pourriels. Et vous éviterez aussi de traîner partout vos 70 comptes Hotmail.

apprendre à utiliser ici, car son nom est quand même bien plus prononçable (de plus, Jack B. Nymble 2 ne fonctionnait pas bien sur ma machine tournant sous XP). Lors de l'installation, il commence par vous demander votre adresse email et votre serveur SMTP habituel, ne soyez pas timide et donnez-lui de vraies infos (au moins pour le serveur), sinon vous risquez d'avoir des problèmes pour envoyer vos mails. Au lancement, il détecte que nous n'avons pas encore installé la librairie de cryptage Mixmaster et nous propose de la télécharger. Pas d'hésitation, cliquons sur "Get Mixmaster 2.9".

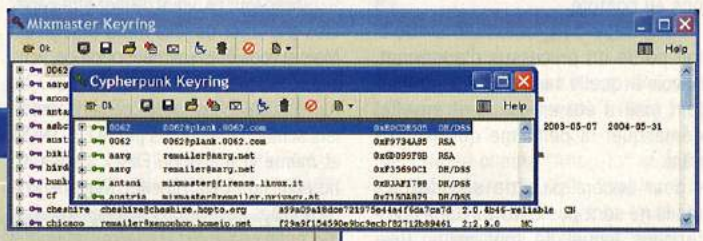


Il se connecte alors sur le FTP de QuickSilver et nous propose de télécharger un des modules : celui qui nous intéresse se nomme "Mix29b39.zip", sélectionnez-le dans la liste et cliquez sur "Next". Après le téléchargement, cliquez sur "Run Setup". Une confirmation de l'installation de Mixmaster s'affiche.



Cliquez sur "Next", choisissez le répertoire d'installation de Mixmaster, "Next","Install", "OK"... on y est presque, il reste à accumuler des données aléatoires, ce qui se fait en traçant des traits à la souris jusqu'à ce que le compteur indique 100%. Ensuite, "Exit", puis "OK", et QuickSilver se lance enfin ! Vous pouvez désactiver la fenêtre "For beta testers only" qui se lance par défaut au démarrage. Bon, il reste encore configurer la bestiole, en commençant par lui rentrer quelques infos sur les remailers. Allez dans Tools / Remailers. Cochez les 4 cases devant "mlist.txt", "publist.mix", "rlist.txt" et "pubring.asc" puis cliquez sur Update. Le programme télécharge automatiquement toutes les infos nécessaires. Cliquez sur OK.

Vous voyez maintenant deux fenêtres, "Mixmaster Keyring" et "Cypherpunk Keyring", contenant les clés Mixmaster et PGP des différents remailers.



Toutes les clés téléchargées automatiquement, c'est bien, mais il est plus prudent de s'assurer que ce sont bien les dernières en les mettant à jour manuellement. Cette technique permet aussi d'utiliser QuickSilver même si les sites avec les clés disparaissent. Pour cela, utilisez la méthode vue plus haut pour demander leur clé aux remailers que vous souhaitez utiliser. Pour chacun d'eux, sélectionnez tout le contenu du mail contenant les clés et copiez-le dans le presse-papier. Cliquez alors avec le bouton droit dans la fenêtre "Mixmaster Keyring", et choisissez "Import...", et enfin cliquez sur "Clipboard". Si le message "NO NEW KEYS" apparaît, cela signifie que vos clés sont à jour, tout va bien. Sinon, vous importerez la nouvelle clé qui apparaîtra dans la liste. Il est temps maintenant d'envoyer notre premier mail mixmaster : dans le menu "File", choisissez "New" puis "Message". Le champ "Host" doit contenir votre serveur SMTP, le champ "From" est presque inutile puisque le remailer le changera, le champ "To" contient bien sûr la destination, et enfin le champ "Chain" indique quels remailers vous voulez utiliser (par exemple "austria,hastio" en spécifiant les noms, ou "*,*,*" pour une chaîne de trois remailers aléatoires, ou "*,austria" pour choisir un premier remailer aléatoirement et spécifier le second comme austria).
(voir image New messafe)

Si vous avez mis à jour les clés manuellement, vous préférerez désactiver l'option "Update on Send" du menu "Tools", qui permet de re-télécharger toutes les clés juste avant d'envoyer un mail, pour être sûr d'être à jour. Vous pouvez maintenant cliquer sur "Send". Si le mail ne veut pas partir et que votre serveur mail est correctement entré,c'est peut-être que le serveur de votre fournisseur d'accès empêche le relais de mails. Dans ce cas-là, lisez l'encadré

LES CD PIRATÉS

CNN rapporte que la vente de CD piratés dépasse un milliard de copies par année. Ce marché vaut environ 0,6 milliard de dollars, une hausse de 7% par rapport à l'an dernier. Les ventes de CD "légaux" ont chuté de 7,2% en 2002. La raison: la trop grande disponibilité de CD piratés, particulièrement dans les pays pauvres, et les mp3. Les pauvres ne peuvent en effet pas acheter les originaux. Où est donc le manque à gagner pour les éditeurs, qui ne veulent pas baisser leurs prix? "Dans les touristes", nous souffle notre ami Billou.

CLONECD BIENTÔT ILLÉGAL

Comme vous le savez tous (comment ça non?), la prochaine loi sur le droit d'auteur rendra toute copie de jeu ou CD illégale, donc CloneCD deviendra un logiciel illégal très bientôt. La version 4.2.0.2 sera peut-être la dernière de ce fameux logiciel, puisque ses concepteurs ne veulent pas aller en prison. Peut-être y aura-t-il une version en ligne de CloneCD, mais seulement en Suisse où l'entreprise compte déménager sous peu. La version en ligne ne pourra pas être utilisée si vous habitez en dehors de la Suisse, où les lois protègent les concepteurs de ce logiciel. Tiens, tout d'un coup, la Suisse va peut-être devenir une destination de choix pour bien des compagnies: toutes les autres entreprises du genre sur le marché (comme VSO chez nous – l'éditeur de BlindWrite et CopyToCD) risquent de devoir cesser leurs activités à la suite de la mise en vigueur de la loi. C'est l'Allemagne qui a sonné le gong de l'offensive, mais les autres pays de l'Union Européenne (France, Grande Bretagne, Italie, Autriche...) devraient suivre très bientôt.

"Installer son propre serveur SMTP".

Un compte email anonyme

Envoyer des mails anonymes, c'est bien, mais que dites-vous d'en recevoir aussi ? La tâche est un peu plus compliquée, car vous devez récupérer vos emails, ce qui implique de se dévoiler. Il existe bien des services de webmail "sécurisés" comme Hushmail (www.hushmail.com) - qui a été utilisé par le groupe DEViANCE par exemple comme adresse de contact dans ses nfos - mais vous pouvez toujours être identifié... Le meilleur moyen de recevoir des mails anonymement est de créer un compte nym, ce que nous allons faire pas à pas dans la suite. Comme pour les remailers Cypherpunk, vous allez avoir besoin de PGP, alors s'il n'est pas encore installé, dépêchez-vous ! Le serveur nym.alias.net est le plus populaire, mais pas le plus rapide d'après mes essais : deux autres serveurs nyms sont redneck.gacracker.org (celui que nous allons utiliser ici) et nym.xganon.com. Commencez par envoyer un email sans sujet ni texte à remailer-key@redneck.gacracker.org. Vous devriez recevoir (bientôt avec un peu de chance, soyez patient...) la clé PGP du serveur, que vous importerez dans vos clés PGP comme auparavant. Ensuite, envoyez un mail à list@redneck.gacracker.org : vous aurez en réponse la liste de tous les alias déjà utilisés sur ce serveur, de façon à ce que vous n'en choisissiez pas un qui existe déjà. En attendant la réponse, nous allons créer notre "reply block", c'est-à-dire le bloc qui va indiquer au serveur nym comment nous envoyer les mails qui nous sont destinés. Pour faire simple, je vais prendre ici l'exemple où vous utilisez simplement le remailer "austria" entre vous et le serveur nym. Commencez par taper les instructions pour diriger les emails vers votre vraie adresse :

```
::
Anon-To: piratgamez@yahoo.fr
Encrypt-Key: piratownz
```

Le champ "Encrypt-Key" est facultatif, mais sert de sécurité supplémentaire : il s'agit d'une passphrase que vous aurez à taper pour décrypter votre message (elle sert à masquer le destinataire du message au cas où le message encrypté serait intercepté). Comme ce bloc est destiné au dernier remailer qui vous enverra les réponses, encryptez-le avec la clé du remailer austria (utilisez la clé RSA Legacy et non la clé DSS, en tout cas c'est plus prudent si vous voulez maximiser les chances que ça fonctionne), cela vous donne dans le presse-papier un bloc que je nomme BLOC1 dans la suite. L'étape suivante est de dire au serveur nym qu'il faudra envoyer le mail à austria, ce qui se fait en tapant :

```
::
Anon-To: mixmaster@remailer.privacy.at
Encrypt-Key: piratownz

::
Encrypted: PGP

BLOC1

**
```

Attention, tous les espaces sont très importants ! Maintenant que le "reply bloc" est prêt (je le note REPLYBLOC dans la suite), il s'agit de formater la requête de création d'alias. Vous allez d'abord devoir vous créer une nouvelle paire de clés PGP pour votre nouvelle adresse. Supposons que nous voulons nous appeler "Piratz <piratz@redneck.gacracker.org>" : dans PGP on choisit "PGPKeys", puis dans le menu "Keys", "New Key...", puis "Expert". Dans "Full Name", il faut mettre "Piratz", et dans "Email address", piratz@redneck.gacracker.org, et enfin dans "Key type" choisir "RSA Legacy" (laisser "Key size" à 2048 et "Key expiration" à "Never"). Faites ensuite un clic droit sur la clé nouvellement créée et choisissez "Copy" pour la copier dans le presse-papiers. Enfin, tapez dans votre éditeur de texte, sans le saut de ligne après "acksend' :

```
Config:
From: piratz@redneck.gacracker.org
Nym-Commands: create +acksend
+signsend name="Piratz"
Public-Key:
```

Et collez votre clé juste en dessous (sans saut de ligne après "Public-Key"). Tapez encore dessous (toujours sans saut de ligne après "Acksend"):

```
Reply-Block:
REPLYBLOC
```

où, pour ceux qui n'ont pas suivi, vous remplacerez bien sûr REPLYBLOC par le bloc que vous avez créé auparavant. Au final, votre email doit ressembler à ça :

```
Config:
From: piratz@redneck.gacracker.org
Nym-Commands: create +acksend
+signsend name="Pirat'z"
Public-Key:
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0.2 - not licensed for
commercial use: www.pgp.com

mQGiBD8QPBORBADY+SYqXHrDKS7I
+J206ZTkYU6VLv34GDYzswRnLQf+b
o5j2wwo
ONSktfwGcya2kBiZvjaIi8DKWIoYim1
1DIe5xjcOMqFfBOdLZqxZLrwaBcp2W
gvm
-----END PGP PUBLIC KEY BLOCK-----
Reply-Block:
::
Anon-To: mixmaster@remailer.priva-
cy.at
Encrypt-Key: piratownz

::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for
commercial use: www.pgp.com

qANQR1DBwE4DTpBM/M97kj4QA/
4o841gy9aFD76Thb7PL+Lnnknjq5M
qw3eDTxSK
C3R++vSayHEkiPtW09oaeX+IH/pZt
M3xnjkCc4/8SZ+hPWvnbJNCw0Hwh
BKEGcoT
-----END PGP MESSAGE-----

**
```

Maintenant, il ne reste "plus" qu'à encrypter tout ça avec la clé du serveur nym que vous avez dû recevoir depuis le temps (dans le cas de redneck.gacracker.org, vous devez avoir deux clés, il faut utiliser celle de config@redneck.gacracker.org) , ET A SIGNER pour prouver que ça vient bien de vous, ce qui se fait tout simplement avec la fonction "Clipboard" / "Encrypt and Sign" de PGP (pensez à bien choisir la nouvelle clé que vous venez de créer pour signer). Vous pouvez maintenant envoyer le contenu du presse-papier à config@redneck.gacracker.org, ce que je vous conseille de faire anonymement par l'intermédiaire d'un ou plusieurs remailers bien sûr !

Avec un peu de chance, vous allez recevoir dans les heures qui sui-

'Z

Un hacker trop gourmand

Un New-Yorkais de 25 ans a été arrêté pour avoir installé un keylogger dans des ordinateurs publics. Pendant plus d'un an, il a ainsi pu espionner les activités de milliers de personnes, interceptant des coordonnées bancaires et des mots de passe. Il a finalement été pris lorsqu'il a eu la mauvaise idée d'utiliser un compte hacké du logiciel GoToMyPC (logiciel pour accéder à un ordinateur à distance) pour contrôler un ordinateur sur lequel quelqu'un était en train de travailler, et qui a relevé son IP. Ce n'était donc pas un lecteur de Pirat'z.

Tous contre la RIAA

À la suite des poursuites intentées contre les partageurs de P2P, les réseaux P2P multiplient les mesures visant à compliquer la vie de la RIAA. Rappelons-nous que celle-ci avait pollué les réseaux avec de faux fichiers (des musiques incomplètes, des vidéos Canal+ sans décodeur, des chansons de Dorothée, enfin rien que des abominations destinées à faire fuir les internautes de KaZaa et Cie). Et bien, cette idée a inspiré iMesh, qui a décidé de lui rendre la pareille en rajoutant de faux ordinateurs sur leur réseau. Ainsi, les sbires de la RIAA traqueront des internautes fantômes partageant des fichiers fantômes avec d'autres internautes fantômes téléchargeant ces fichiers fantômes... bon je crois que vous avez compris le principe. "Il s'agit du virus contre l'antivirus, du firewall contre le hacker" a déclaré le PDG de iMesh. "Pour chaque nouvelle mesure, il y a une contre mesure, et à la fin de la journée, personne n'y a gagné." Enfin, pas tout à fait: dans ces deux exemples, c'est généralement le méchant qui gagne. Reste à savoir ici qui est le méchant.

vent une réponse cryptée. Si vous recevez immédiatement une réponse, c'est généralement mauvais signe, il y aura sans doute marqué quelque chose du genre " Could not decrypt message". Dans ce cas-là, vérifiez que vous aviez bien encrypté votre mail avec la bonne clé, et que votre clé publique perso est bien du type RSA Legacy, de même que celle du remailer vous avez utilisé (sinon je ne réponds de rien). D'autre part, n'importe quelle erreur, aussi minime soit-elle (un espace en trop ou en moins), risque de tout foutre en l'air et vous ne recevrez jamais un message vous indiquant ou est l'erreur exactement. Enfin bref, si tout va bien vous voici avec une réponse cryptée, que vous allez décrypter avec PGP : la "passphrase" demandée au début (deux fois dans notre cas) est "piratownz", et la dernière est celle de la paire que vous avez créée pour l'occasion. Dans ce mail, vous trouverez une adresse à laquelle il faut envoyer un email (n'importe quoi, peu importe) pour activer définitivement votre alias. Evidemment, il est conseillé d'envoyer ce mail via un remailer...

La dernière étape : envoyer un email à l'aide de votre nym tout neuf. Tapez votre email avec la syntaxe suivante :

From: piratz
To: concurrent@demerde.com
Subject: Attention

Nous sommes là !

Encryptez ça avec la clé de send@redneck.gacracker.org, puis signez-le, et envoyez le tout (toujours via un ou plusieurs remailers bien sûr) à send@redneck.gacracker.org. Et voilà, le tour est joué !

Sachez qu'il existe encore d'autres astuces pour le mail anonyme (comme l'utilisation de newsgroups pour récupérer ses mails en toute discrétion), mais nous attendrons peut-être un prochain numéro pour en parler !

LE PEER-TO-PEER

Avec les actions récentes de la RIAA contre des usagers de Kazaa, sans compter les lettres qu'ont pu recevoir certains abonnés français suite à des plaintes d'associations de lutte contre le piratage, et la menace Retspan qui plane toujours, l'anonymat sur les réseaux P2P revêt beaucoup d'attraits, non pas pour dissimuler vos activités illicites (qui n'existent pas de toute manière), mais surtout pour au moins avoir enfin la paix. Nous vous avions déjà parlé un peu du problème de l'anonymat dans le Pirat'z numéro 2 : pour résumer, il s'agit d'un challenge compliqué, car pour se cacher il faut introduire des intermédiaires (comme les remailers pour le mail), ce qui ralentit forcément le débit... Le projet Freenet (http://www.freenetproject.org/) continue tranquillement son développement, et pourrait s'avérer une solution viable à terme. Par contre son objectif est clairement l'anonymat avant la performance, ce qui le rend peu pratique pour les gros fichiers, et se traduit aussi par des fonctions de recherche très basiques, ce qui n'est quand même pas la joie. Filetopia (www.filetopia.org) est un autre réseau orienté vers l'anonymat, avec encryption des données. Par contre, pour cacher son IP, il faut passer par des "bouncers", qui sont l'équivalent de proxies : non seulement il vous faudra vous-mêmes dénicher un bouncer, mais en plus à moins de connaître personnellement la personne qui le fait tourner, comment pouvez-vous être sûr qu'elle ne va pas justement s'amuser à vous espionner ? Ce n'est décidément pas ce qu'il y a de mieux, alors voyons ce qu'Earth Station 5 (www.earthstation5.com) peut nous proposer : encryption (des transferts et sur disque grâce à pgpDisk), utilisation de l'UDP au lieu du TCP/IP, blabla, mouais... Ohoh, "serveur proxy", qu'ils annoncent, en un seul clic de souris ! Tout alléché, j'installe la bête, malgré un mauvais pressentiment dû au look horrible de leur page web. Pressentiment qui se confirme en voyant à quoi ressemble le programme (je vous ai mis une photo d'écran pour vous faire partager ce bijou).

Après avoir cherché longtemps avant de trouver qu'il fallait cliquer sur "Alignement" pour accéder aux options, je découvre qu'il faut chercher soi-même des serveurs proxies, et que donc le programme n'offre rien de plus que les autres dans ce domaine. Allez zou, direction la poubelle, et je passe à Blubster (www.blubster.com), qui annonce depuis sa version 2.5 un anonymat total. Par contre, impossible de trouver les spécifications détaillées de la technologie, ce qu'ils doivent sans doute justifier par la nécessité de protéger leurs secrets révolutionnaires, mais depuis quand quelqu'un dési-

INSTALLER SON PROPRE SERVEUR SMTP

Parfois, le serveur de mail de votre fournisseur d'accès est configuré pour vous empêcher certaines fonctions : par exemple il peut ne pas accepter de relayer des emails (fonction utilisée par QuickSilver), ou ne pas fonctionner avec un programme comme Ghost Mail. Dans un tel cas, il peut être utile d'installer soi-même un petit serveur SMTP sur sa machine afin de pouvoir envoyer des emails sans passer par le serveur de son provider. Il existe de nombreux serveurs, et notamment un gratuit sous Windows s'appelle Postcast Server et peut se télécharger sur : http://www.postcastserver.com/html/download.asp. Après l'installation, qui ne pose pas de difficulté particulière, lancez le programme, qui affiche le "Setup Wizard". Cliquez sur "Next", puis cochez (en tout cas je vous le conseille) la case "Allow access only from users with these IP addresses", et n'autorisez que votre propre IP (127.0.0.1) à envoyer des mails (sinon vous risquez de voir quelqu'un envoyer des mails à partir de votre ordinateur, ce qui pourrait vous causer des ennuis). Cliquez sur "Next", et choisissez d'envoyer les messages "Immediately". Cliquez enfin trois fois sur "Next", puis sur "Finish". Pour utiliser votre serveur de mail tout neuf, vous devez spécifier le serveur smtp "127.0.0.1". Par exemple, dans QuickSilver, la ligne "Host" doit être : Host: 127.0.0.1. Si vous remarquez que vos mails ne partent pas, c'est peut-être que votre fournisseur bloque le port 25 en sortie (ce que de plus en plus font, pour bloquer les spammers). Dans ce cas, il n'existe malheureusement que peu de recours : utiliser une autre machine à laquelle vous avez accès pour relayer les messages, ou employer par exemple le service "Mail reflector" de no-ip.com, qui coûte quand même 40 $ / an...

MICROSOFT TALONNE SONY DE LOIN

Microsoft a annoncé avoir vendu plus de consoles que prévu au cours du second trimestre 2003. Pendant ce temps, les ventes de PS2 progressent moins vite... est-ce la fin de la domination de Sony ? Pas vraiment : il y a encore plus de 5 fois plus de PS2 dans le monde que de Xbox, il est donc normal que les ventes de PS2 ralentissent, tout le monde en ayant déjà une. Les bons résultats de la Xbox sont imputés à la qualité des jeux (hmm), à la baisse du prix (mouais), et selon nous, aux nouvelles possibilités de piratage.

LINUX EST-IL ILLEGAL ?

C'est en tout cas ce que s'efforce de démontrer SCO, un développeur de système Unix, qui maintient que le noyau (kernel) de Linux à partir du 2.4 contient du code "volé" de leur propre système d'exploitation, "Unix System V". A partir de ces accusations (qui restent à prouver), SCO entend bien se remplir grassement les poches en faisant cracher les utilisateurs de Linux. En effet, SCO a entrepris de contacter les entreprises dont le parc informatique est sous Linux, afin de leur proposer un marché: acheter une licence "UnixWare" leur autorisant à exécuter les programmes Linux, en échange d'un généreux oubli de leur infraction passée. Sinon, c'est direction le tribunal. Evidemment, nombreux sont ceux qui doutent de la réalité de la menace SCO: un professeur en droit a ainsi déclaré que même si du code avait effectivement été copié, les simples utilisateurs ne pouvaient être accusés de violation du droit d'auteur. On peut aussi se demander si ce code n'est pas issu d'un produit Linux GPL de SCO... qui se serait ainsi tiré une belle balle dans le pied:-)

rant rester anonyme ferait confiance à boîte noire magique ? J'ai définitivement renoncé à l'installer (et je vous recommande d'en faire autant) en découvrant que le programme venait avec quelques petits spywares sympathiques comme l'ami Gator. Sachant que Blubster ne permet en plus de ne télécharger que des fichiers musicaux, on peut passer, il n'y a pas grand-chose à voir. Si vraiment vous voulez l'essayer, téléchargez au moins une version sans spywares, à cette adresse par exemple : http://drdamn.com/cleanclients/blubster250.shtml.

Finalement, les réseaux P2P sont encore loin d'être à la hauteur au point de vue anonymat, même si des efforts sont faits. Si vous deviez vraiment choisir aujourd'hui, je vous conseille encore Freenet, qui paraît être le projet le plus sérieux. Une autre source d'inquiétude vient de la légalité de tels réseaux. On pourrait en effet penser que puisque tout est encrypté et que Freenet n'a aucun contrôle possible sur le contenu du réseau, il ne peut pas être tenu responsable de ce qui y transite. Ce n'est malheureusement pas forcément vrai : le 1er juillet, la RIAA a en effet remporté une victoire légale qui pourrait s'avérer importante contre le réseau P2P Madster (anciennement Aimster). Ce dernier avait déjà perdu l'an dernier, mais avait fait appel en disant qu'il ne pouvait être tenu pour responsable de ce qui transitait sur son réseau : puisque tout était crypté, comment savoir que c'était illégal? "Vous deviez vous en douter", a dit en gros le juge. Qui, il faut bien l'avouer, n'avait pas tout à fait tort sur ce coup-là...

Une autre option consiste à se protéger spécifiquement des enquêtes de la RIAA et des autres associations anti-piratage en bloquant les adresses IP qu'ils utilisent. Le programme PeerGuardian (http://methlabs.org/methlabs.htm) est justement fait exactement pour ça. Un autre outil utile est le convertisseur disponible sur http://www.bluetack.co.uk/convert.html qui permet de convertir les listes de blocage d'IP d'un format à un autre, pour les adapter à tous les principaux logiciels de P2P. La fonction de blocage d'IPs de la RIAA est même maintenant intégrée à la dernière version de Kazaa Lite (www.kazaalite.tk), le célèbre clone de Kazaa (sans les pubs et spywares). Mais ne pensez pas que bloquer ces IPs vous rend invisible et vous donne le droit de faire ce que vous voulez sur le réseau : pendant que vous bloquez des IPs, les associations anti-piratage en acquièrent d'autres, ou mettent la main sur des proxies pour contourner le blocage. Et à ce jeu du chat et de la souris, c'est forcément la souris qui finit par se faire prendre.... Alors certes, il y a beaucoup plus de souris que de chats et il y a peu de chances que ce soit vous, mais réfléchissez-y bien avant de prendre le risque !

Il y a bien une méthode plus sûre pour protéger votre identité, mais au détriment des performances : il s'agit bien sûr du proxy. La plupart des clients P2P permettent en effet de passer par un proxy - fonction présente à la base pour permettre la connexion depuis un réseau d'entreprise par exemple - mais que vous pouvez utiliser à votre avantage pour camoufler votre IP. Par exemple, sur le populaire eDonkey, cela se règle dans le menu "Options", puis "Proxy". Les proxies les plus populaires sont les proxies de type "Socks 4" ou "Socks 5" (voir l'encadré sur les types de proxies). Par contre, utiliser un proxy présente deux inconvénients majeurs : la rapidité tout d'abord (ça risque de ramer sévèrement), et le fait d'être connecté indirectement au réseau, ce qui se manifeste sous eDonkey par exemple par un "low ID", ce qui implique des possibilités un peu plus limitées (voir le Pirat'z numéro 2 pour plus de détails sur les "low ID"). Bref, l'anonymat en P2P est possible, mais il faut en payer le prix !

Il vous faut au moins cocher la case "Server" pour vous connecter au serveur via le proxy. Encore une fois, vous utiliserez le plus souvent les classiques proxies Socks 4 et 5, avec un risque cependant : de nom-

I.R.C.

C'est bien connu, votre maman vous l'a dit, le réseau IRC regorge de violeurs d'enfants, de psychopathes schizophrènes et de lecteurs de Pirat'z mal intentionnés. Dans ces conditions, éviter d'afficher trop visiblement notre véritable identité est parfois une sage précaution. En effet, sous EFnet par exemple, vous pouvez obtenir des infos sur quelqu'un par la commande :

/whois nick

qui renvoie quelque chose du genre :

nick is lili@modem205.53-131-66.nowhere.videotron.ca * lili
nick on #piratz
nick using irc.homelien.no Who Cares
nick End of /WHOIS list.

Et on a facilement son adresse IP par :

/dns nick

qui renvoie :

*** Looking up modem205.53-131-66.nowhere.videotron.ca
*** Resolved modem205.53-131-66.nowhere.videotron.ca to 66.140.24.37

Bon, ça, c'est ce que vous voulez éviter que les autres apprennent sur vous. Le moyen le plus courant est d'utiliser un proxy (pour changer), ce qui se configure sous mIRC dans les options, onglet "Firewall".

'Z

Après l'Angleterre, l'Allemagne

C'est au tour de l'Allemagne d'adopter la loi pour interdire les courriels commerciaux indésirables et ainsi renforcer la lutte contre le spam. Cette loi obligera les entreprises procédant de cette façon à verser leurs profits à l'État. La ministre allemande de la protection du consommateur suggère aux internautes de choisir leur fournisseur internet en fonction de la protection contre cette publicité non désirée plutôt qu'en fonction du prix : les fournisseurs ne donnant pas de protection contre la pub ne pourront rester sur le marché!

ZoneLoader Unloaded

On vous annonce dans l'article sur la PS2 l'arrivée prochaine du ZoneLoader, un CD de boot permettant en théorie de jouer aux sauvegardes de jeux sans modchip, avec tous les jeux et toutes les versions de PS2. Pas de chance, les responsables du projet ont annoncé sur www.ps2ownz.com qu'ils rencontraient des difficultés imprévues, et que le ZoneLoader était retardé AU MOINS jusqu'à Noël. Autant dire qu'il ne faut pas trop compter dessus, et que les modchips et autres Swap Magic ont encore de beaux jours devant eux.

Surfer sur sa PS2

Normalement, le service en ligne fourni avec la Playstation 2 ne permet que de visiter les pages "made in Sony". Il fallait s'y attendre, il est en réalité possible de surfer sur la globalité du réseau, et ce de manière relativement simple: il suffit de modifier l'adresse par défaut à laquelle se connecte la console. La manip', qui ne fonctionne que sur les consoles européennes, est décrite sur le site de celui qui l'a découverte : www.brookfresh.co.uk/default2.htm. A quand un buffer overflow dans le browser de la PS2 qu'on rigole un peu?

breux serveurs n'acceptent pas les proxies et vous renverront un message "banned" lors d'une tentative de connexion. Il n'y a pas grand-chose à faire dans ce cas, sinon essayer un autre serveur du même réseau... Une fois connecté, pensez à faire un /whois sur vous-même pour vérifier que le proxy a bien été configuré.

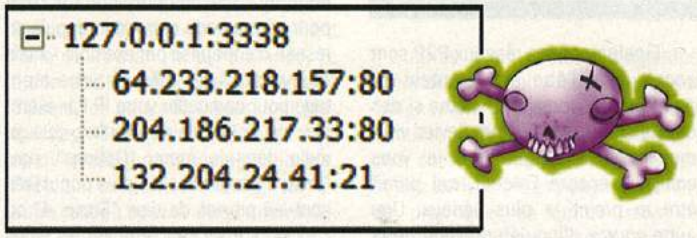
Certains réseaux IRC offrent des fonctions d'anonymat pour protéger votre adresse. Vous pouvez généralement le découvrir dans le texte d'accueil du serveur ou en fouillant sur le site web du réseau, mais il n'y a pas de règle générale à ce sujet, et vous devrez chercher par vous-mêmes. Enfin, une méthode classique utilisée sur IRC pour se camoufler est l'emploi d'un shell (un compte sur une machine – généralement Unix/Linux) pour se connecter au serveur. La plupart de ceux qui utilisent un shell le paient (il existe de nombreux sites offrant des shells pour un prix raisonnable, je vous laisse chercher sur Google), ce qui leur permet d'installer dessus un "bouncer" (ou bnc en abrégé), qui est une sorte de proxy pour IRC. L'avantage est qu'ils peuvent ainsi être connectés 24h/24 par le shell, sans être forcément connectés sur leur propre machine. Cette méthode est quand même assez complexe, un peu coûteuse, et ne vous protège évidemment pas de tout puisque la personne qui vous loue le shell sait très bien qui vous êtes ! Un des avantages indéniables est quand même de pouvoir choisir parmi tout plein de noms de domaines très sexy, du genre piratz.owns.ze.world.com.

LE FTP

Le FTP est un autre domaine où l'anonymat n'est pas aisé, car on souhaite souvent obtenir un taux de transfert rapide, ce qui limite l'usage de proxies. C'est pourtant la meilleure solution pour l'anonymat. Prenons l'exemple de celui qui est sans doute le meilleur client FTP entièrement gratuit, SmartFTP (www.smartftp.com) : les proxies s'activent dans le menu "Tools / Settings / Connection / Proxy".

METTEZ PLUSIEURS PAIRES DE CHAUSSETTES

SocksChain (http://www.ufasoft.com/socks/) est un programme extrêmement utile pour tout internaute parano qui se respecte. Il permet en effet de créer simplement des "chaînes" de proxies : grâce à lui, vous pouvez mettre entre vous et votre cible autant de proxies intermédiaires que vous le souhaitez, ce qui permet de s'assurer d'un anonymat confortable (il faudra beaucoup de temps à une personne très motivée pour remonter une piste de plusieurs proxies depuis les quatre coins du monde). Je vous indique rapidement comment utiliser ce petit outil : la première chose à faire est d'aller dans "Tools / Proxy Manager" et de cliquer sur "Update list" pour télécharger la dernière liste de proxies, puis "Test all" pour les vérifier. Ceci fait, fermez le proxy manager puis cliquez sur "Service / New". Dans "Accept connections on Port" je vous conseille de mettre autre chose que 1080 pour plus de sécurité. Vous pouvez laisser les autres options identiques ("Change the chain every" permet de spécifier au bout de combien de temps le programme modifie automatiquement la chaîne pour plus de sécurité, "Chain length" spécifie une longueur de chaîne, et enfin si vous le souhaitez vous pouvez choisir quels proxies vous voulez exactement utiliser, mais je vous laisse bidouiller ça par vous-mêmes). Après avoir cliqué sur OK, la chaîne est activée et il suffit de configurer votre logiciel (mIRC par exemple) avec comme proxy un proxy Socks (4, à moins que vous n'utilisiez que des Socks 5 dans la chaîne), à l'adresse 127.0.0.1 et sur le port que vous avez spécifié (1081 par exemple). Lorsque vous vous connectez, vous devriez voir en haut à droite de la fenêtre de SocksChain une petite arborescence qui montre les connexions en cours, comme dans la capture ci-dessous.



GOOGLE A PERDU LA CLEF!

Ça va mal pour Google: le populaire moteur de recherche serait sur le point d'avoir de sérieux ennuis. Il pourrait bientôt atteindre le nombre maximum de pages indexées. En effet, les URL sont codées sur une clef de 4 octets, ce qui donne 4,294,967,296 pages pouvant être indexées. De plus, pour certains termes on retrouve déjà pratiquement 4 milliards de pages. Pour régler ce problème il faudrait augmenter la taille de la clef: mais quoi que fasse Google, ce qui est sûr c'est que ça va leur coûter cher en serrurier!

NOUVEAU DANS LE PEER-TO-PEER?

Il y a sans doute parmi vous des nouveaux venus dans le monde fantastique du Peer-to-Peer (P2P, si vous ne saviez pas de quoi il s'agissait partout dans ce numéro), qui se sentent un peu perdus au milieu de tous les termes et tous les logiciels différents: un document de synthèse serait le bienvenu... Souhait exaucé avec la parution d'un dossier assez complet sur le sujet, dispo sur www.open-files.com/site/dossier/page71.htm. Et si vous préférez le PDF, il est sur www-igm.univ-mlv.fr/~duris/NTREZO/Peer-to-peer.pdf. Merci aux auteurs!

ZONEALARM: TO PATCH OR NOT TO PATCH

That is ze big question qu'a dû se poser Zone Labs, les créateurs de ZoneAlarm, le firewall personnel le plus populaire. En effet, une vulnérabilité a été trouvée, permettant à un programme d'accéder à des sites web sans permission préalable. Le hic: les développeurs ont d'abord estimé que protéger la version gratuite de ZoneAlarm était trop compliqué... ce que les médias se sont empressés de dénoncer. Un peu honteux, ils ont fait marche arrière, et ont commencé à travailler sur le patch. Ça ira pour cette fois, les gars...

LES DIFFÉRENTS TYPES DE PROXIES

Vous êtes perdus entre Socks, HTTP, ports 3128 à 8080, etc ? Pas de panique, Pirat'z est là pour éclaircir tout ça. Les proxies "classiques" pour le web sont les proxies HTTP, qui sont utilisés par un navigateur web comme IE. Ces proxies ne sont à la base pas prévu pour autre chose, et sont presque toujours sur les ports 8080 ou 3128 (mais aussi parfois 80, ce qui est moins courant dans le cas d'une configuration "normale"). Les proxies Socks, eux, sont plus récents et sont utilisés dans beaucoup plus d'applications, car ils permettent de faire passer n'importe quel trafic TCP/IP, voire UDP pour les Socks dits de type 5 (qui sont une évolution des Socks 4, donc plus perfectionnés). Les proxies Socks se dénichent presque toujours sur le port 1080. Et voilà, c'est tout ce que vous avez à savoir pour commencer à vous aventurer dans le monde merveilleux des proxies !

Vous remarquerez qu'il y a différents types de proxies. Les plus classiques pour le FTP sont nos bons vieux amis Socks (4 et 5, laissez tomber le 4a), ainsi que les proxies dits "FTP" du type "USER user@host:port". Cette syntaxe signifie que lorsqu'on utilise le proxy, on lui demande de nous connecter par exemple au serveur ftp.piratz.com sur le port 2121 sous le nom d'utilisateur "khan" par la commande :
USER khan@ftp.piratz.com:2121.

Il existe différentes syntaxes selon les proxies, c'est pour cela qu'il y a plein de choix dans SmartFTP, vous aurez à expérimenter pour trouver le bon.

Evidemment, utiliser un proxy a l'inconvénient habituel de limiter sérieusement notre bande passante. De plus, en téléchargeant à travers le proxy, vous augmentez les risques de voir le proxy fermé à cause d'un débit trop important. Une solution intermédiaire consiste à vous connecter sur le serveur par le proxy, mais à télécharger directement, grâce au FXP ! Ainsi, l'adresse IP visible par l'administrateur du serveur FTP (celle logguée par le serveur) sera celle du proxy, tandis que les fichiers iront directement sur votre machine sans passer par le proxy. Pour ceci, vous devez faire du FXP (transfert de serveur à serveur), ce qui se fait en installant un serveur FTP sur votre machine, en vous connectant d'un côté sur le serveur FTP distant par le proxy, de l'autre sur votre serveur local sans proxy, et en lançant un transfert FXP entre les deux (pour plus de détails, voir le Pirat'z numéro 1, ou chercher un peu sur le net des tutoriaux sur le FXP). Cette technique n'est évidemment pas parfaite côté anonymat puisque votre adresse IP reste visible, une connexion TCP/IP directe s'établissant entre vous et le serveur FTP. Mais si personne ne surveille, vous passerez sans doute inaperçu à moindres frais...

LE CYBER-CAFÉ, L'ARME ULTIME POUR L'ANONYMAT ?

Malgré tous les efforts que vous pourrez déployer, dans bien des cas, il sera toujours possible de remonter jusqu'à vous en retraçant l'origine des connexions, c'est-à-dire votre adresse IP (même si celle-ci est enfouie au fond d'obscurs logs de proxies), ou votre numéro de téléphone. Dans ces conditions, se connecter à partir d'un cyber-café est une solution attrayante pour ceux qui veulent être absolument intraçables (n'oubliez pas d'éviter quand même les caméras de surveillance, encore que ça risque de paraître louche dans un cybercafé, un client en lunettes de soleil devant son ordinateur). Evitez aussi toute activité pouvant mener vers vous : je me souviens qu'un hacker chevronné a ainsi déjà été pris parce qu'il avait consulté son email (sur une messagerie type Hotmail) à partir du même cybercafé d'où il avait hacké quelques machines du Pentagone. Mais en prenant de bonnes précautions, c'est sans doute un bon moyen de minimiser les risques. Evidemment, le cyber-café n'est quand même pas la solution idéale : non seulement c'est cher, mais en plus rien ne vous dit que le client précédent ne vient pas d'installer un keylogger sur la bécane que vous utilisez...

COMMENT SCANNER ?

Déjà, pour les petits nouveaux, rappelons que scanner consiste à "examiner" un ordinateur pour déterminer quels sont les services qu'il offre. Bien que légale en théorie, cette pratique est souvent considérée comme illégale car étant la première étape d'une tentative de hacking (après avoir scanné et trouvé un logiciel tournant dessus, on peut essayer d'exploiter une faille de ce logiciel pour hacker la machine). Enfin bref, sachez que si vous scannez, votre fournisseur d'accès vous fera peut-être parvenir un jour une lettre vous demandant d'arrêter, et là je vous conseille d'obéir ;) En attendant, scanner permet de découvrir des proxies pour vous tout seul (donc potentiellement rapides). Vous pourrez trouver plusieurs scanners spécialisés dans les proxies en cherchant "proxy scanner" dans google. Pour les flemmards, en voici un par exemple : http://www.proxybench.com/proxy/socks-checker.asp. Généralement, vous devrez spécifier un intervalle d'adresses IP à scanner, et le programme fera le reste. Je vous conseille d'éviter les adresses d'universités, qui sont reconnues comme très peu douillettes quand on les chatouille avec un scanner (ce qui signifie que ça ne les fait absolument pas rigoler). Et vous savez quoi ? Lorsque vous scannez, vous avez intérêt à passer par un proxy, afin de scanner anonymement !

'Z

PROTESTATION ANTI-RIAA

À la suite des poursuites que veut intenter la RIAA contre les gens téléchargeant des mp3, il y aura une série de protestations un peu partout aux États-Unis. En effet, un groupe contestataire a prévu de descendre dans la rue le 2 août afin de manifester son mécontentement ainsi que son désaccord vis-à-vis de l'industrie de la musique américaine. Ce groupe veut être entendu par les 5 compagnies de disque les plus importantes, par la RIAA et le Congrès. Il va leur falloir chanter fort, car ces derniers ont l'oreille plutôt dure...

VIRTUAL JAGUAR SORT, ET S'ARRÊTE!

L'émulateur Jaguar (si si, souvenez-vous, la console d'Atari dont le nom évoque la rapidité avec laquelle on l'a oubliée) Virtual Jaguar s'est fait beaucoup attendre... et est enfin sorti sur potato.emu-france.com! Par contre, son auteur, après avoir bien bossé sur cet émulateur, a décidé de passer à autre chose, et a donc arrêté le projet. Heureusement, il a eu la bonne idée de le distribuer sous la licence GPL, et un clone multi plates-formes peut déjà se télécharger sur sdlemu.ngemu.com. Et non, je n'ai pas de ROMs pour vous!

SPAMMEZ FACILE GRÂCE À NET SEND

Dans le numéro 3, nous vous expliquions pourquoi vous receviez sans arrêt des messages publicitaires sous XP, et comment vous en débarrasser (pour ceux qui l'ont raté, une solution rapide consiste à désactiver le service d'affichage des messages). Mais maintenant que vous avez bien souffert, il est temps de vous venger! Si vous vous sentez l'âme d'un programmeur, vous pourrez envoyer des messages anonymes via le service de messages, grâce par exemple au code dispo sur http://www.codeproject.com/useritems/anetsend.asp.

LES METIERS DE LA

Dans le numéro précédent, nous vous avions fait découvrir le passionnant "métier" de Siteop. Aujourd'hui,nous allons nous intéresser à celui de Trader (synonyme de "courier"), sans doute le plus représenté sur la Scène pirate. Mais avant toute chose, un court rappel s'impose pour ceux qui ont raté le dernier épisode....

DUR DE RÉPARTIR 99 CENTS

Si vous avez lu attentivement toutes les news de votre magazine préféré, vous savez que les artistes veulent vendre leurs singles sur le net plus de 99c. Et bien selon une étude, il ne resterait pratiquement plus rien aux artistes une fois tout payé. Effectivement, 40c reviennent au site qui distribue le single, puis 30c à la maison de disque pour les droits d'auteur, 8c pour l'éditeur, les autres distributeurs comme AOL reçoivent 10c, et il reste donc plus qu'un gros 11c pour l'artiste. Bref, c'est pas mieux que pigiste chez Pirat'z.

JOUER EST DANGEREUX

Non, il ne s'agit pas d'une énième victime des jeux vidéo, ayant succombé à une trop longue partie de Counter Strike. Ceux-là, on ne les compte plus, vous pensez bien. Nous parlons ici d'une nouvelle vulnérabilité "critique" (pour que Microsoft consente à la qualifier de critique, vous pensez bien que c'est pas de la rigolade) affectant toutes les versions de DirectX de la 5.2 à la 9.0a (donc pas la dernière, la 9.0b), et ce sur toutes les versions de Windows. Il s'agit d'un buffer overflow (quelle originalité) dans le code gérant les fichiers MIDI (vous savez, ce format de fichier musical utilisé dans tous les vieux jeux, même les plus récents (un jeu avec ses musiques en MIDI, même récent, est déjà vieux)). Un fichier MIDI formaté d'une manière spéciale pourrait donc exécuter du code arbitraire camouflé dans le fichier. Même s'il n'y a pas d'exploit connu à cette date, vous feriez mieux de protéger votre machine en la patchant par Windows Update, en installant le dernier DirectX, ou même – conseil de Pirat'z avisé – en repassant sous DirectX 3!

Et oui, désolé pour nos lecteurs réguliers qui connaissent déjà tout ça, mais notre nombre de lecteurs triplant dans le monde à chaque seconde, il faut bien prendre en compte les petits nouveaux. Je vais quand même essayer d'être bref... La Scène pirate (ou Warez), c'est le monde underground où des milliers d'internautes s'échangent les derniers logiciels, films, mp3 et cie (piratés bien sûr). Ces programmes sont mis à la disposition du public par des groupes, qui les distribuent au départ sur de gros serveurs FTP très rapides (10, 100, 200, 1000 Mbits et plus). Ces serveurs FTP sont appelés des "Sites", et sont gérés par des personnes appelées les "Siteops". Une fois qu'un logiciel est disponible sur un site, ceux qui y ont accès s'empressent de le transférer sur tous les autres sites sur lesquels ils ont un compte (car ces sites sont bien sûr extrêmement privés). On assiste donc à un phénomène de distribution progressive du logiciel piraté sur le réseau : par exemple, un jeu de 650 Mo va être disponible sur les meillleurs sites moins d'une minute après avoir été sorti par un groupe, tandis que les sites plus "bas de gamme" vont devoir attendre quelques heures, voire quelques jours... et les utilisateurs de eDonkey, eux, quelques semaines le temps de finir le téléchargement ;)
Les internautes transférant les "releases" (logiciels piratés) entre les différents sites sont appelés des "traders", ou "couriers". Ceci vient de ce que dans ce petit monde, rien n'est gratuit : pour avoir le droit de télécharger quelque chose sur un site, il faut consommer des crédits (exprimés en Mo), qui ne se gagnent qu'en uploadant. Ainsi, un trader qui transfère le jeu X (650 Mo) du site A vers le site B perd 650 Mo de crédits sur A, mais en gagne (le plus souvent) 650 x 3 = 1,95 Go sur B. Un trader doit donc savoir bien gérer ses crédits, sous peine de se retrouver à court...

Pour en savoir plus, nous avons déniché un trader qui a accepté de nous parler de sa "profession". Car, comme vous allez le voir, être trader peut être un travail à temps plein !

PIRAT'Z : Salut
TRADER : 'Lu

PIRAT'Z : Peux-tu nous en dire un peu plus sur toi ? Ton âge, ton sexe, ton travail ?
TRADER : Je ne peux pas trop en dire, mais ça ça devrait aller, on ne devrait pas pouvoir me retrouver... J'ai 22 ans, je suis un homme - comme 99,9% des personnes dans la Scène - et je suis encore étudiant.

PIRAT'Z : La journée typique d'un trader, c'est quoi ?
TRADER : Hmm... je commence par me lever, pour me rendre compte qu'il est trop tard pour aller en cours. J'allume alors mon ordinateur (si je l'avais éteint), puis je vaque à mes occupations. Et dès qu'une release est là, je saute devant ma bécane pour la trader [= transférer une release entre deux sites]. Généralement, je me couche assez tard :)

PIRAT'Z : Et comment sais-tu qu'il y a une nouvelle release ?
TRADER : Oh, comme tous les traders, j'ai un système d'alarme. Je suis présent en permanence sur les canaux IRC de mes sites [= ceux auxquels ils à accès], et dès que le bot [= client IRC automatique qui sert ici à annoncer les nouvelles releases] fait une annonce, mon ordi me prévient.

PIRAT'Z : Est-il vraiment indispensable d'être averti à la seconde près ?
TRADER : Oh oui ! Tous les sites ont une limite en nombre d'utilisateurs connectés en même temps, et si tu arrives trop tard, le site est plein... Tu as un joli message tel que "Site is full... Try again later". Et adieu les crédits ! D'autre part, la plupart des courses ["races" en anglais] ne durent que quelques minutes tout au plus, et partir le premier peut faire une grosse différence.

PIRAT'Z : Est-ce que tu peux détailler un peu plus ce que sont ces "courses" ?
TRADER : Oui, bien sûr. Tu n'es jamais le seul à uploader une release sur un site : d'autres traders sont en compétition avec toi, et celui qui uploade le plus de fichiers (en Mo) gagne la course. Gagner une course n'est pas indispensable pour les crédits, mais c'est une bonne partie du fun pour les traders. Et ça fait mieux paraître ton groupe.

PIRAT'Z : Il y a donc un classement systématique ?
TRADER : Oui, tu veux un exemple ?

PIRAT'Z : Bien sûr !
TRADER : Tiens, voici un compte-rendu d'une course :

Rank	Courier	Team	Files	Size (kb)	Percentage
01.	xxx	P****	12	175776	42.1
02	yyyyyyy	S**	8	117184	28.1
03	zzzzzzz	A*****	8	109543	26.3
04	uuuuuu	E*****	1	14648	3.5
Rank	**Team**	**Best Courier**	**Files**	**Size (kb)**	**Percentage**
01.	P****	xxx	12	75776	42.1
02.	S**	yyyyyyy	8	117184	28.1
03.	A*****	zzzzzzz	8	109543	26.3
04.	E*****	uuuuuu	1	14648	3.5
04 racer(s) / 04 group(s) Files: 29 417151 kb 100.0					

SCENE : LE TRADER

[Les véritables noms ont été supprimés pour respecter leur anonymat]
Tu as d'abord le classement individuel, puis le classement par groupe. Ici, c'est évidemment le même car les 4 traders qui ont pris part à course étaient dans 4 groupes différents.

PIRAT'Z : Ces groupes, quels sont-ils exactement ?
TRADER : Ce sont des "curry groups" [groupes de traders], c'est-à-dire des équipes de personnes qui passent leur temps à trader des releases entre les sites. Lorsqu'un groupe se montre à son avantage sur certains sites, en gagnant les courses et en uploadant plus que les autres, il peut espérer gagner accès à d'autres sites plus prestigieux, où ils seront en compétition avec d'autres groupes plus difficiles à battre.

PIRAT'Z : Un peu comme les divisions en sport alors ?
TRADER : Un peu, sauf que les divisions ne sont pas clairement établies. Il n'y a pas de sites "de division 1" et d'autrres "de division 2", du moins pas officiellement.

PIRAT'Z : Y-a-t-il des risques à être un trader ?
TRADER : Dès que tu mets un pied dans la Scène, il y a des risques que tu dois accepter. Les traders, même s'ils ne fournissent pas eux-mêmes le matériel piraté, ont leur part de responsabilité dans la distribution de celui-ci. Un trader risque gros s'il est pris...

PIRAT'Z : Pourquoi prendre ces risques, alors ?
TRADER : Parce qu'au fond, c'est un passe-temps tellement prenant qu'on en oublie ces risques. Il y a tellement de traders dans le monde, pourquoi moi ? Et puis, être trader donne accès à pas mal de logiciels pour rien, ce qui est un avantage non négligeable. Je dirais que les traders les plus menacés sont quand même ceux des "gros" groupes, donc la plupart des petits traders ne se sentent pas non plus vraiment en danger.

PIRAT'Z : Et toi, prends-tu des précautions particulières ?
TRADER : Autant que je peux. Malheureusement, il est difficile pour un trader de se protéger, car l'accès aux sites est protégé par un système de vérification d'IP, ce qui empêche de bien se camoufler. La meilleure protection consiste encore à choisir soigneusement les sites sur lesquels on est, car si le site se fait prendre, la police n'aura aucun mal à trouver notre IP. Les sites US en général présentent plus de risques car les américains sont ceux qui ont fait le plus d'efforts contre ce type de piratage. J'évite aussi les sites hébergés dans les universités, qui font de plus en plus attention à l'utilisation de leur bande passante.

PIRAT'Z : As-tu déjà été pris, ou as-tu déjà failli te faire prendre ?
TRADER : Non, heureusement. J'ai déjà été sur des sites "à risques" (US, universités), mais je les ai abandonnés depuis. Ça ne vaut pas le coup de risquer la prison.

PIRAT'Z : Sur combien de sites es-tu, au fait ?
TRADER : Actuellement, seulement 6. Mais j'ai déjà été sur bien plus, du temps où j'étais plus actif. Ces 6 sites sont ceux affiliés à mon groupe.

PIRAT'Z : Oh, tu fais partie d'un "release group" alors ? [= groupe piratant les logiciels, contrairement aux "curry groups" qui ne font que les trader]
TRADER : Oui, je m'occupe d'uploader nos releases sur nos sites. Par contre, je ne te dirai pas quel est ce group ni de quel genre de release il s'agit ;)

PIRAT'Z : Et ça prend beaucoup de temps, ce travail ?
TRADER : Ça dépend... moi, je pourrais me contenter de seulement uploader nos releases, ce n'est pas trop fatiguant. Mais pour être un bon trader, il faut y mettre beaucoup de temps, afin d'être là sur toutes les releases. Les meilleurs traders passent généralement au moins la journée devant leur ordinateur, et parfois même mettent des alarmes la nuit pour être sûrs de ne rien manquer !

PIRAT'Z : Je vois, c'est presqu'aussi fatigant que rédacteur à Pirat'z... Et à part ça, les traders ont-ils une vie ?
TRADER : Héhé, pas toujours. Mais certains trichent, avec l'auto-trading : ils installent des scripts sur leur ordinateur pour qu'il transfère les releases à leur place, pendant qu'eux sont à 10 km de leur bécane. Evidemment, l'auto-trading est très mal vu, car les traders ne veulent pas être en compétition avec une machine.

PIRAT'Z : As-tu déjà fait de l'auto-trading ?
TRADER : Non, mais j'ai déjà utilisé des scripts se connectant automatiquement aux sites lorsqu'une nouvelle release arrivait. Ça, c'est permis. Enfin, il me semble ;) De toute manière, l'auto-trading est dangereux car on risque de se faire prendre. Certains groupes s'amusent à sortir des "fausses" releases pour voir si quelqu'un va la trader : si c'est le cas, il s'agit sans doute d'un auto-trader...

PIRAT'Z : Et au fait, comment es-tu devenu trader ?
TRADER : J'ai commencé plutôt bas dans l'échelle, sur les boards FXP [voir Pirat'z numéro 1]. Là, j'ai eu la chance de me lier avec un gars qui s'est avéré être plutôt haut placé dans la Scène, et qui plus tard m'a proposé de devenir trader pour son groupe. J'ai eu de la chance, mais c'est souvent ainsi qu'on rentre dans la Scène : tout est question de savoir se faire apprécier par les bonnes personnes.

PIRAT'Z : Que penses-tu de Kazaa, eDonkey et Cie ?
TRADER : Je ne sais pas trop... D'un côté, comme beaucoup de personnes dans la Scène, je trouve que les réseaux P2P sont en grande partie responsables de l'attention portée par la police à nos activités. Si seulement le petit monde de la Scène avait accès aux releases pirates, on nous laisserait sans doute tranquilles. En ce sens, la démocratisation du piratage fait beaucoup de mal au piratage. D'un autre côté, je comprends ceux qui militent pour une Scène moins "élitiste", où tout le monde pourrait avoir ce qu'il veut gratuitement. Mais au total, il ne faut pas oublier que ce sont les éditeurs qui y perdent le plus, et le piratage de masse ne peut pas continuer ainsi sans dégâts irrémédiables pour l'industrie. Je dis donc "mort au P2P" ;)

PIRAT'Z : Un dernier mot, sur la disparition récente de Fairlight ?
TRADER : Ah, c'est sûr qu'ils vont me manquer. Je respectais beaucoup ce groupe, qui a toujours fait preuve de professionalisme dans ses actions. C'est donc inquiétant de voir qu'ils ont préféré arrêter, mais je les comprends. Et, après tout, la Scène du jeu PC n'est pas morte pour autant, d'autres groupes ont repris le flambeau.

PIRAT'Z : Et bien, merci Mr. Trader, et ne manque pas le prochain Pirat'z !
TRADER : Je voudrais bien, mais je ne l'ai pas dans mon pays !

LE PLUS GRAND PIRATE FRANÇAIS ARRÊTÉ

Enfin, c'est l'impression que l'on a lorsqu'on voit les commentaires de la presse sur l'arrestation d'un " hacktiviste " français, grand défaceur devant l'éternel. Ce dernier avait l'habitude de pirater régulièrement des sites web afin de faire passer son opinion politique sur la situation au Moyen-Orient. Cette activité avait comme seule conséquence de rappeler à leur devoir les administrateurs web. Il est pourtant soudainement devenu un pirate dangereux pour la police, toute fière de l'avoir identifié. Bravo Messieurs, le net est plus sûr grâce à vous !

MICROFLAW

Encore un faille parue juste trop tard pour apparaître dans notre revue, mais qui y aurait largement eu sa place: mi-juillet, une vulnérabilité a été découverte dans un composant de Windows servant à effectuer des requêtes à distance (RPC = Remote Call Procedure). Cette faille est déjà assez sérieuse puisqu'il s'agit d'un buffer overflow, autorisant l'exécution de code arbitraire donc la prise de contrôle totale de l'ordinateur à distance. Autre point qui la fout plutôt mal pour Microsoft: toutes les versions récentes de Windows (NT 4.0, 2000, XP, et surtout 2003 Serveur, le système le plus sécurisé de la marque) sont vulnérables. Cette vulnérabilité peut être exploitée en envoyant un message spécialement formaté sur le port 135: un moyen rapide de s'en protéger est donc de s'assurer de bien configurer son firewall pour bloquer ce port (un patch est également disponible). Car il vaut mieux s'en protéger: le groupe de sécurité chinois Xfocus (www.xfocus.org) a en effet publié un exploit qui pourrait bientôt donner lieu à un ver type Code Red...

L'ACTU DES MODCHIPS SUR PS2

Les modchips (ou puces) sur Playstation 2 n'en finissent plus de se succéder. Suite à l'article paru dans le numéro précédent, un lecteur nous a justement fait remarquer que nous ne parlions pas de la Ripper 2... Puce sortie en effet peu de temps après la rédaction de l'article. Nous allons donc tenter ici de faire un petit point (non exhaustif) sur les dernières nouveautés dans le domaine sur PS2.

'IZ

LE P2P AU BUREAU, C'EST PAS BEAU!

Une entreprise canadienne, AssetMetrix, a fait une étude sur l'utilisation des logiciels P2P dans les sociétés canadiennes. Dans les 560 entreprises ayant répondu au sondage, plus de 70% des sociétés possédaient au moins un ordinateur connecté à un réseau de P2P. De plus, une firme possédant plus de 500 ordinateurs a "automatiquement" un logiciel de P2P. Cette entreprise canadienne avait une solution à proposer aux sociétés sondées: AssetMetrix vend un logiciel permettant de détecter les logiciels de P2P sur un réseau ;)

FAITES-VOUS PAYER POUR UTILISER KAZAA!

Malgré toutes les actions menées par la RIAA à son encontre, Kazaa se porte encore bien, merci. Evidemment, ses créateurs commencent quand même à sentir le feu se rapprocher dangereusement de leurs fesses, et afin de sauver leur peau tout en continuant à se remplir les poches, tentent de mettre en avant le côté "légal" de Kazaa. Ce côté, encore peu connu du grand public, se nomme Altnet, et se caractérise par le fait qu'il s'agit d'une partie intégrante de Kazaa, mais payante: le but d'Altnet est de distribuer des produits payants en P2P, ce qui aurait pour avantage de légitimer Kazaa. L'inconvénient, bien sûr, c'est que ça marche moins bien que le "côté obscur" de Kazaa, qui reste gratuit et bien plus fourni en mp3 et autres goodies. La nouvelle idée d'Altnet pour se populariser: rémunérer les internautes qui participeraient à la distribution payante et légale de logiciels, films et musiques. D'après leur PDG, "les procès sont le bâton, notre approche est la carotte". Reste à savoir si celle-ci sera suffisamment appétissante pour avoir du succès...

SANS MODCHIP, C'EST PLUS CHEAP

Commençons par rappeler qu'un modchip n'est pas obligatoire pour pouvoir jouer à vos copies (de sauvegarde) de vos jeux. Les solutions sans modchip ont l'avantage de ne pas avoir à ouvrir (ou faire ouvrir) sa console, ce qui maintient la garantie et évite les erreurs de soudure parfois fatales. L'inconvénient : elles sont moins pratiques pour jouer, et ne fonctionnent pas toujours parfaitement.

Les premières solutions sans modchip impliquaient des techniques relevant du bidouillage pour pouvoir éjecter un CD sans que la console le remarque (voir par exemple le Pirat'z numéro 2). Aujourd'hui, des méthodes moins compliquées (mais plus chères) existent, notamment le "Slide-Card" et le "Flip-Top", qui sont deux accessoires que l'on monte sur sa PS2 pour faciliter le changement de CD ("swap"). D'après les premiers utilisateurs de ces deux méthodes, le Slide-Card serait un peu plus dangereux (plus de risques d'abîmer sa console) si manipulé un peu trop brusquement : si vous en achetez un, allez-y donc doucement...

Dans tous les cas, sans modchip vous aurez besoin d'un CD de boot ("boot disc") que vous échangerez avec le CD auquel vous voulez jouer. Le CD le plus efficace est sans doute le "Swap Magic", les deux concurrents étant le DVD Région X et l'Action Replay 2. Dans tous les cas, renseignez-vous bien avant d'acheter pour vous assurer qu'il est compatible avec votre modèle de PS2 (V3 à V8, je ne vais pas encore vous redonner les instructions pour le déterminer, vous les trouverez ici par exemple : http://www.ominfo.com/plans/versions/versionsps2.html).

Mais attention, tous les jeux ne fonctionnent pas avec le Swap Magic et ses amis. Vous trouverez une liste des jeux non compatibles ici : http://www.ps2ownz.com/forums/showthread.php?s=&threadid=2825. Ce problème est en partie corrigé avec le CDLoader, une image CD à graver et qu'on peut télécharger gratuitement sur http://www.hostultra.com/~liamv/. Malheureusement, ce programme ne

fonctionne que sur les PS2 jusqu'à la V6, donc si vous avez un modèle plus récent, il faudra attendre le ZoneLoader (www.zoneloader.com), pas encore sorti mais qui s'annonce comme un remplacement au Swap Magic capable de faire tourner tous les jeux (il sera payant, comme le Swap Magic). Comme il n'existe pour l'instant qu'à l'état de promesse, pensez à faire un tour sur les forums pour vérifier ce que les utilisateurs en pensent avant d'acheter.

Enfin, tous ces CD de boot sont aussi parfois utiles avec un modchip dit "sans fil", c'est-à-dire sans soudure. Ces modchips servent essentiellement à remplacer les techniques de swap hasardeuses (ce que font déjà le Slide-Card et le Flip-Top). Leur installation est par contre plus compliquée que celle de ces derniers. Si vous voulez en savoir plus sur ces modchips, visitez www.badben.fr.st qui y est consacré.

LES DERNIERS MODCHIPS

Passons maintenant aux modchips, aux vrais, ceux qui se soudent sauvagement au cœur de votre PS2, faisant sauter la garantie quand ce n'est pas votre console. Les meilleurs sur le marché sont toujours le Messiah 2 et la DMS 3 (pour cette dernière, il faut prendre la version 2, une petite amélioration de la première version). Leurs deux concurrents les plus récents sont la Ripper 2 et la F14. La Ripper 2 se hisse à leur niveau, avec des fonctionnalités à peu près identiques. Vous pouvez donc a priori craquer pour celle-ci, même si personnellement j'aurais tendance à attendre encore un peu pour s'assurer que tout va bien. En tout cas, si vous l'achetez, une des premières précautions semble être de s'assurer que la puce ne rentre pas en contact avec la tôle de la console : un certain nombre de personnes ont eu des problèmes à cause de ça, problèmes réglés tout simplement en rajoutant par exemple un bout de scotch entre la puce et la tôle.

Le cas de la F14 est par contre plus délicat : il s'agit d'une toute nouvelle puce, pas encore largement utilisée, et qui n'a pas autant de fonctionnalités que ses adversaires. Vu son prix pas forcément plus attractif, son avantage principal semble se réduire à une installation un peu plus simple. Un avantage assez réduit qui m'amène donc à ne pas vous la conseiller pour l'instant, sauf si la soudure vous fait vraiment peur et que vous voulez minimiser les risques de bavure.

RESTEZ AU COURANT

Il est difficile à un magazine comme le nôtre de vous tenir au courant des toutes dernières nouveautés, puisque nous sortons moins vite que les modchips ;) Le meilleur moyen si vous souhaitez rester à la pointe du progrès est de visiter les sites et forums dédiés à la PS2 :

- http://www.ominfo.com/forum : le forum d'Ominfo, auquel on pourra juste reprocher d'orienter parfois les conversations vers leurs propres produits
- http://jcinfos.fr.st : le forum d'Assentek, fermé au moment où nous bouclons, mais gardez un œil dessus
- http://www.ps2ownz.com : c'est en anglais et donc les discussions concernent plus souvent les consoles US, mais vous y trouverez tout de même beaucoup d'infos, et pourrez voir venir ce qui arrive depuis l'autre côté de l'Atlantique !

Quoi qu'il en soit, nous vous parlerons bien sûr de toute avancée importante des modchips sur PS2, en espérant que la loi ne nous l'empêche pas évidemment ;) Alors, en attendant le prochain numéro, bonne soudure, bon jeu, et pensez à ACHETER des jeux, et pas uniquement des CD vierges...

LA XBOX ENTIEREMENT CRACKEE

L'an dernier, Michael Robertson, le père de LindowsOS, mettait en jeu 200.000$ pour qui parviendrait à faire tourner Linux sur Xbox. Les premiers 100.000$ sont allés à ceux qui ont réussi ce pari sur une Xbox équipée d'un modchip. La somme restante a servi à motiver la communauté pour réussir à trouver une solution SANS modchip, et ceci avant décembre 2003 (date de remise des récompenses). Petite revue des dernières méthodes à ce jour... ET ATTENTION : toute manipulation de votre console est dangereuse pour sa santé. Hacks à consommer avec modération.

James Bond vient à la rescousse

La première solution purement logicielle a été trouvée à la fin mars. Il s'agit d'exploiter une vulnérabilité de type "buffer overflow" dans la gestion des sauvegardes du jeu "007 Agent Under Fire". En créant une sauvegarde bidon formatée de manière spéciale, il est possible d'exécuter du code arbitraire sur la console, donc en particulier de lancer Linux. Le fichier de la sauvegarde peut se télécharger sur : http://xbox.xbox-linux.com/down/007linux.txt (ouvrez ce fichier texte avec Winrar par exemple pour décompresser la sauvegarde). Toute la difficulté consiste ensuite à transférer cette sauvegarde sur votre Xbox. Cela peut se faire de différentes manières :

- en utilisant une Xbox déjà hackée pour copier la sauvegarde sur son disque dur, puis du disque dur vers une carte mémoire (ou un périphérique de stockage USB, que la Xbox est aussi capable de lire, à l'aide un adaptateur USB)
- en utilisant un PC sous Linux capable d'écrire au format de fichier FATX (le format de la Xbox), afin d'écrire sur un périphérique USB que la Xbox pourra lire. Ce n'est pas très simple car vous devrez recompiler votre kernel Linux. Des instructions détaillées se trouvent sur : http://www.xemulation.com/forums/viewtopic.php?t=4. On peut trouver sur le net (sur IRC notamment, essayer #xlinux et #xbins sur EFnet, mais je ne vous promets rien, et qui sait, peut-être qu'eDonkey...) un fichier nommé xlinux-1.2c.rar qui contient déjà une distribution Linux toute prête pour ça.
- avec un peu de chance, vous trouverez l'image au format FATX de la sauvegarde, et vous n'aurez qu'à en faire une copie brute sur un périphérique USB. Bonne recherche !
- enfin, vous pouvez ouvrir votre Xbox, brancher son disque dur sur votre PC, et copier la sauvegarde dans le répertoire UDATA. De cette manière vous n'avez besoin ni de carte mémoire, ni de périphérique USB. Par contre, c'est assez dangereux puisque vous ouvrez votre console... Un tutorial sur comment connecter son disque dur Xbox sur son PC se trouve par exemple ici : http://forums.xbox-scene.com/index.php?act=ST&f=45&t=73720

Pour lancer Linux, il suffit alors de lancer 007 et de charger la partie hackée.

Un exemple de périphérique / carte mémoire USB pour ces manip' est le Mega X-Key, sur lequel vous trouverez plus de détails ici : http://207.44.176.77/~admin28/emuxbox/articles/megaxkey.htm

Microsoft nous aide aussi

Le 23 juin, un nouveau jeu permettant le même type d'exploit a été dévoilé : il s'agit de MechAssault, un jeu de... Microsoft ! Son principal intérêt par rapport à 007 est que le jeu est reconnu comme bien meilleur ;) Les étapes sont les mêmes, et vous trouverez le code de la sauvegarde sur http://www.xbox-hacker.net/forums/index.php?act=ST&f=12&t=11849 (lisez bien les discussions dans ce thread, ça pourra vous aider).

Plus besoin de jeux !

Gros inconvénient de la méthode ci-dessus : vous devez toujours commencer par lancer un jeu, ce qui est fatigant à la longue. Mais le 4 juillet, le groupe Free-x a divulgué un autre exploit tirant parti d'une vulnérabilité dans le dashboard de la Xbox (l'utilitaire qui se lance lorsqu'aucun jeu n'est inséré). L'exploit a été dévoilé sur cette mailing-list : http://lists.netsys.com/pipermail/full-disclosure/2003-July/010895.html

Pour utiliser cet exploit, il faut par contre remplacer des fichiers du dashboard, ce qui nécessite soit d'utiliser une fois le hack de la sauvegarde pour lancer Linux et remplacer les fichiers, soit de brancher le disque dur de la Xbox sur votre PC (voir le lien donné plus haut). De cette manière, Linux pourra se lancer à chaque démarrage de la console. J'ai comme l'impression que 007 et MechAssault vont avoir du succès dans les boutiques de location de jeux...

La méthode Flash

Encore une autre solution consiste à flasher le Bios pour le remplacer par un Bios "spécial Linux", qui lancera Linux systématiquement. Mais c'est une méthode plus délicate, car vous devrez souder 2 ponts sur votre console (la méthode est décrite sur http://www.xbox-scene.com/articles/tsop.php). De plus, attention car ensuite les jeux ne se lanceront plus !

Quand les pirates s'en mêlent

Toutes ces recherches ont évidemment été faites dans le but de faire tourner Linux sans modchip, mais si Linux peut tourner, pourquoi pas une copie de jeu ? C'est ce que s'est dit le groupe Complex, qui a sorti ainsi deux "loaders" capables de faire tourner les jeux copiés sur une Xbox non modifiée ! (non, inutile de nous le demander, nous ne savons pas où le trouver). Le premier est une version modifiée du hack pour 007 Agent Under Fire. Le second une version modifiée du hack du dashboard. Ce dernier a pas mal de fonctionnalités, avec par exemple une détection automatique PAL / NTSC !

Autre technique détournée, le flash du Bios permet bien sûr d'installer un Bios spécial Linux, mais aussi un Bios de modchip comme le bios "Xecuter 2", ce qui permet de faire tourner toutes les sauvegardes comme si le modchip était effectivement installé ! Un guide complet sur comment flasher son bios se trouve sur http://forums.xbox-scene.com/index.php?act=ST&f=43&t=61901.

Tout ceci fait évidemment le bonheur des pirates, et risque de poser de sérieux problèmes à Microsoft. On peut logiquement penser qu'ils essaieront de rectifier le tir sur les prochains modèles de Xbox à être mis en vente, mais le mal est déjà fait : avec plus de 9 millions d'unités écoulées (ce qui est moins que prévu, au passage), la majorité du parc est vulnérable à un simple hack software. La seule bonne nouvelle pour Billou est qu'installer un tel hack est encore relativement compliqué pour les débutants. Le jour où il sera possible de créer des copies de jeux se lançant toutes seules sur une Xbox non modifiée, ça risque de faire très mal à la crédibilité de la console pour les développeurs de jeux. Et alors, il ne nous restera plus que Linux pour jouer !

On a retrouvé Nemo sur le Net

Une des techniques favorites des pirates pour copier un film dès sa sortie en salle consiste à le filmer pendant la projection (ou même avant, s'ils ont accès aux bobines du film). Les studios essaient donc d'empêcher l'introduction de caméras et autres camescopes. Mais les détecteurs de métaux à l'entrée ne suffisent pas toujours: Disney a ainsi fait travailler des agents de sécurité équipés de lunettes de vision de nuit pour empêcher le piratage de "Finding Nemo". Résultat: le film est sorti sur internet le jour-même de sa sortie en salle.

COURRIER DES LECTEURS

Comme d'habitude, vos chagrins d'amour sont à nous confier sur piratgamez@yahoo.fr. Avant de nous écrire, vérifiez que votre question n'est pas dans la FAQ: 1) je veux une adresse illégale (moi aussi) 2) je veux m'abonner (moi aussi, mais ce n'est pas possible pour l'instant) 3) je veux un ancien numéro (moi je les ai, je les vends 1000 euros pièce) 4) je veux votre site internet (moi je veux que tu me le fasses) 5) je veux coucher avec vous (moi non, je suis hétéro). Merci !

Je voulais juste vous envoyer un petit mot pour vous remercier de votre magazine que je trouve original et excellent. J'aime surtout vos articles pour leur clarté et l'humour du rédacteur !!!!!
Merci l'équipe de PIRAT'Z, vous êtes géniaux ;-)
PS : Suis une fille, vous voyez y a même des filles qui lisent votre magazine lol :-)

ELFE JOYEUSE

Aaaarg... voilà qui fout en l'air ma réponse 5)

Ayant acheté votre dernier mag (que j'ai beaucoup apprécié), j'ai regardé la section anti-clic droit, et je tenais à vous dire que j'ai découvert un moyen de passer cette protection. Voilà la soluce (attention, pour ceux qui ont l'ADSL, ça va être dur!) : lorsque la page commence à se charger, c'est-à-dire lorsqu'il n'y a pas la totalité, faites un clic droit, normalement, vous devriez avoir le menu, mais il faut être rapide si la page se charge rapidement ! Après, vous verrez à quel moment vous devrez faire le clic, question de feeling (enfin...). Voilà, c'était juste pour dire ça. Et continuez votre mag, il est génial !

NESSUS

Félicitations, mais ça a l'air de demander pas mal de doigté. Au passage, un autre lecteur qui se reconnaîtra (si si Michel, tu te rappelles ?) nous a signalé que l'anti-clic droit ne fonctionnait pas non plus sous Opera 6.05. Mais ça, c'est facile de l'éviter, il suffit de faire un site web non compatible avec Opera ! Enfin, l'ami Cyber-Flat nous suggère d'aller récupérer les fichiers que l'on veut garder dans le dossier "Temporary Internet Files" de Windows (si on suppose qu'on a besoin du clic droit pour sauvegarder une image par exemple).

Bonjour, je voudrais savoir comment je me sers de NetBrute pour les 3 parties (NetBrute, PortScan et WebBrute), mais surtout pour la troisième car je ne sais pas exactement comment faire.

SIMON50

Le mieux c'est d'aller voir directement sur la page web du programme : http://www.rawlogic.com/netbrute/. Tout y est expliqué en détail. Par exemple, dans "User File" tu dois mettre un fichier contenant les noms d'utilisateurs que tu veux tester, et dans "Password File" un fichier de dictionnaire de mots de passe. Evidemment c'est toi qui dois fournir ces fichiers. Un lien pour les mots de passe est fourni sur le site : http://www.rawlogic.com/password/wordsall.txt. Pour les noms d'utilisateurs, si tu n'en as aucune idée, tu peux utiliser le même dictionnaire, mais alors ça va ramer... Il vaut mieux avoir une idée des comptes à cracker.

Comment pourrais-je mettre un chat sur mon site HTML ?

L'INCONNU(E)

Tu insères le code : <img src="http://www.didyouknow.cd/animals/graphics/cat.jpg">

Là tu vas me prendre vraiment pour un nul pire qu'un script-kiddie mais il faut vraiment que je sache ce qu'est un cookie et ce qu'est un port, upload et PHP.

@L@B@M@

Comme dit le sage, il n'y a pas de questions stupides, seulement des élèves stupides. Euh, non, oublie ça, aucun rapport. Pour les cookies, voir Pirat'z numéro 2, pour les ports, voir Pirat'z numéro 3. Upload : transfert de données dans le sens contraire du download (téléchargement). PHP : langage de programmation web (voir www.phpfr.org/docs/faq_2.php). Tous ces mots sont également définis sur le dictionnaire en ligne www.dicofr.com.

Bonjour, je lis votre revue avec beaucoup de plaisirs. Malheureusement, je ne suis pas très doué en informatique, alors je me contente des brèves. Il y a quelques jours, un gus m'a royalement viré d'un salon en faisant apparaître un écran bleu sur mon ordi (vous me direz, avec Windows, il y a des chances que cela arrive souvent). Mais là, non, il me prévenait à chaque fois que je revenais et hop – écran bleu - il utilisait - pour le peu qu'il m'en ait dit - un punt ou punter ou un log qui pouvait virer les gens comme cela pff !!!!!!! Si par hasard vous connaissiez ce log ou l'url ou je pourrais le trouver (lui où un autre qui ferait la même chose) j'en serais presque à vous tomber dans les bras et ce afin de lui rendre la pareille.
Merci d'avance et continuez à me délivrer des infos sympa !

BLACKHARMS

Je suis content que tu lises notre revue avec tant de "plaisirs" que ça. Après tout, s'il te suffit des brèves pour te ré-jouir, tant mieux :-)
Bon, a priori, le gars utilise un logiciel de type "nuker", qui permet effectivement de faire planter des ordis à distance, en exploitant des bugs du système. Pour s'en protéger, plusieurs solutions. Déjà, mettre Windows à jour (via Windows update). Ensuite, utiliser un programme de protection, comme "Nuke Nabber" (mais on dirait qu'il n'est plus continué), ou ProPort (http://download.com.com/3000-2381-10133486.html?tag=lst-0-6). Enfin, le mieux, c'est d'installer un firewall et de le configurer correctement, en bloquant les ports utilisés pour te nuker (soit le firewall détectera la tentative de nuke, soit il te faudra aller regarder dans les logs après le plantage pour voir quel port a été utilisé). Tu peux tester ta machine sur winnuke : www.jtan.com/resources/winnuke.html. Des nukers, il y en a plein, mais beaucoup de pages ont des liens brisés. A toi de faire quelques efforts en cherchant sur Google... (un indice quand même : cherche smbdie). Mais c'est mal de vouloir se venger. Le petit Jésus ne serait pas content. Remarque, à mon avis, Jésus ne nous lit pas, il est trop occupé avec Playb... euh, "Histoire du Christianisme", je veux dire.

Je voulais vous demander si vous connaissiez un site où l'on peut trouver un émulateur PS2.
Le Nuker

Il te suffit d'aller fouiner sur un des sites d'émulation donnés dans notre best-of du net. Le plus prometteur pour l'instant est PCSX2 (www.pcsx2.net), mais il est encore loin d'être capable de faire tourner des jeux commerciaux. Au fait c'est toi qui embêtes Blackharms ?

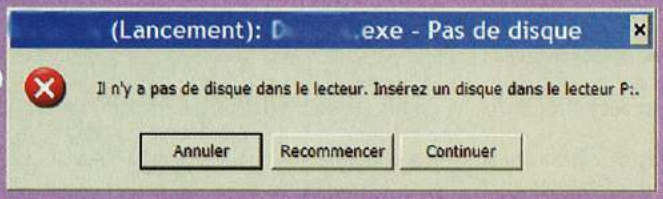
Salut la c un virus a coup sur lol mais fais pas foirer ton ordi quand meme. Bon noel meme si on est en ete.

Dur parfois de s'occuper du courrier des lecteurs...

CRACKER LES CD-CHECKS

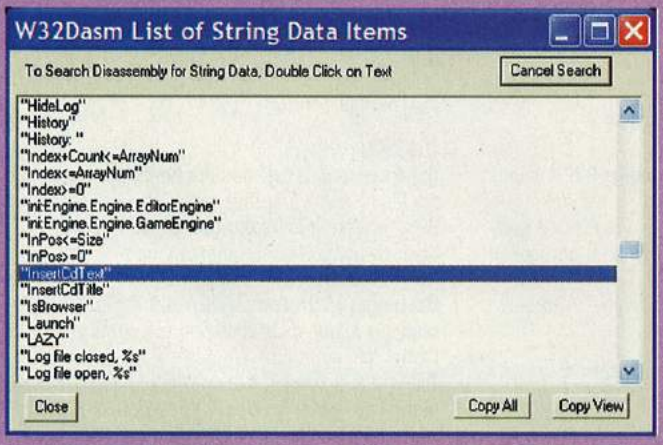
Dans le dernier numéro, nous vous expliquions le fonctionnement des protections CD, et nous vous montrions une technique pour cracker SafeDisc. C'était quand même une entreprise assez ardue, et pour cette raison nous allons voir ici une méthode plus simple destinée à éliminer les "CD-checks" présents dans certains jeux.

Tout d'abord, qu'est-ce qu'un CD-check ? Il s'agit d'un petit bout de code dans le jeu, destiné à vérifier que vous avez bien inséré le CD dans le lecteur. La raison pour laquelle il peut être utile de les supprimer est qu'il rapidement pénible de devoir insérer le CD du jeu alors que tout est installé sur notre disque dur. La plupart des jeux récents étant protégés par une protection commerciale, la technique que nous allons voir risque de ne pas fonctionner sur ceux-ci. Par contre, sur des jeux plus anciens, elle peut être bien pratique. L'exemple que nous allons voir a été réalisé sur un jeu utilisant le moteur d'Unreal, et la présence d'un CD-check se manifeste par l'avertissement suivant lorsque le CD est absent au moment du lancement :



La première chose est de télécharger le désassembleur W32dASM, par exemple ici : www.downseek.com/download/21279.asp. Décompressez-le dans un répertoire quelconque et lancez-le. Faites ensuite une copie de sauvegarde du fichier exécutable de votre jeu (par précaution). Supposons que le nôtre s'appelle tutu.exe. Dans W32dASM, cliquez sur "Disassembler" / "Open File to Disassemble" et choisissez tutu.exe. Si comme chez moi, vous voyez plein de caractères bizarres, rectifiez la police dans le menu "Disassembler" / "Font". Vous voilà devant le code assembleur du programme (vous pouvez vous rafraîchir la mémoire au sujet de l'assembleur dans le numéro 3, ou chercher un tutorial sur le net, mais ce n'est pas complètement indispensable ici).

L'idée est de chercher dans le code du programme où se fait le test de la présence du CD, pour le désactiver. Un bon point de départ consiste à chercher dans les "String Data References" (menu "Refs"), pour chercher une référence vers le message d'erreur demandant d'insérer le CD. Si nous parcourons attentivement la liste, nous trouvons la chaîne "InsertCdText", qui pourrait bien être ce que nous cherchons !



En double-cliquant sur "InsertCdText", W32dASM nous amène sur la portion de code correspondante. Si on regarde les références trouvées par W32dASM juste au-dessus, on voit : "Window" et "InsertCdTitle" avant "InsertCdText", puis plus bas un appel à la fonction "MessageBoxW". C'est donc le bon endroit : le programme crée une boîte de dialogue, puis l'affiche. Le test de la présence du CD doit logiquement se trouver juste avant. Un petit coup d'œil nous permet de voir le code suivant :

```
Reference To:
Core.?GFileManager@@3PAVFFileManager@@A, Ord:02D7h
:1090BA68 8B15547C9510    mov edx, dword ptr [10957C54]
:1090BA6E 8B02            mov eax, dword ptr [edx]
:1090BA70 8B10            mov edx, dword ptr [eax]
:1090BA72 FF5208          call [edx+08]
:1090BA75 898520F9FFFF    mov dword ptr [ebp+FFFFF920], eax
:1090BA7B 83BD20F9FFFF00  cmp dword ptr [ebp+FFFFF920],
                                                00000000
:1090BA82 7F6F            jg 1090BAF3
:1090BA84 6A00            push 00000000

Possible StringData Ref from Data Obj ->"Window"
                          |
:1090BA86 6828CE9210      push 1092CE28

* Possible StringData Ref from Data Obj ->"InsertCdTitle"
                          |
:1090BA8B 68C0D59210      push 1092D5C0

Reference To: Core.?LocalizeGeneral@@YAPBGPBDPBG1@Z,
Ord:03ECh
                          |
:1090BA90 FF15607B9510    Call dword ptr [10957B60]
:1090BA96 83C40C          add esp, 0000000C
:1090BA99 89851CF9FFFF    mov dword ptr [ebp+FFFFF91C], eax
:1090BA9F 6A00            push 00000000

Possible StringData Ref from Data Obj ->"Window"
                          |
:1090BAA1 6828CE9210      push 1092CE28

Possible StringData Ref from Data Obj ->"InsertCdText"
                          |
:1090BAA6 68B0D59210      push 1092D5B0
```

Il vous suffit de savoir que la commande "jg" est un saut conditionnel (c'est-à-dire, si une certaine condition est remplie, alors sauter à tel endroit du programme, sinon continuer). La commande "jg 1090BAF3" fait donc un saut plus loin sous une certaine condition. Puisque le code qui suit sert à afficher une fenêtre que l'on soupçonne d'être celle demandant d'insérer le CD, on en déduit que cette condition est "si le CD est bien présent". Pour enlever le CD-check, il suffit donc de remplacer ce saut par "jmp 1090BAF3", c'est-à-dire "saute toujours, même si le CD n'est pas présent". Cela se fait en éditant tutu.exe avec un éditeur hexadécimal (par exemple HexWorkshop - www.hexworkshop.com). Commencez par repérer où se situe le code à changer. Dans W32dASM, sélectionnez la ligne contenant le saut et regardez tout en bas de W32dASM, il y a marqué quelque chose du genre :

Line:24273 Pg 282 and 283 of 1057 Code Data @:1090BA82 @Offset 0000BA82h in file:tutu.exe

C'est le chiffre après @Offset (ici BA82, le h signifiant juste hexadécimal) qui nous intéresse. Vous pouvez maintenant quitter W32dASM, ouvrir tutu.exe dans HexWorkshop et aller à la position BA82. Dans notre cas le code correspondant est "7F6F", ce que nous changeons en "EB6F" (pour la conversion instructions / code, voir par exemple www.assembly.host.sk/tute/instruc.htm). On recharge le fichier dans W32dASM, histoire de vérifier que la nouvelle ligne est bien :

```
:1090BA82 EB6F            jmp 1090BAF3
```

Et maintenant, il ne reste plus qu'à lancer le jeu... et blam, il accepte de se lancer ! Enfin, je vais être honnête, j'ai un peu simplifié la présentation pour éviter de trop compliquer les choses : dans mon cas, j'avais deux boîtes de dialogue, et je n'ai supprimé ici que la seconde, ce qui fait que je dois cliquer plusieurs fois sur "Annuler" avant que le jeu se lance. Mais bon, il se lance sans CD, et c'est là l'essentiel ! Et puis, de toute manière, c'était juste pour vous apprendre la méthode, puisqu'une solution plus simple consistait à éditer le fichier .ini de mon jeu pour éditer la variable contenant le chemin du CD ;-)

Le Best-of du net Pirat'z

Voici une sélection des meilleurs liens parus dans Pirat'z. Ces sites sont donnés pour information seulement, du contenu potentiellement illégal pourrait s'y trouver suivant la législation de votre pays. Pour notre belle France, voir les articles du code de la propriété intellectuelle relatifs aux logiciels : www.legalis.net/legalnet/cpilog.htm

HACKING et SECURITÉ INFORMATIQUE

iSecureLabs. Actualité en français sur le hacking et la sécurité : www.isecurelabs.com
Packetstorm. Tous les exploits, outils, failles... en anglais : packetstormsecurity.nl
K-Otik. Toutes les vulnérabilités, en français : www.k-otik.com
Input Output Corporation. Une team qu'on l'aime bien : www.ioc.fr.st
Anonymat. Se cacher sur le net : www.anonymat.org
Stay Invisible. Si vous cherchez un proxy : www.stayinvisible.com
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
Zone-H. Actualité des activités pirates : zone-h.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
Tenka.fr.st. Un site en français autour du hacking : www.tenka.fr.st
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
Dicofr.com. Un dictionnaire des termes techniques en informatique : www.dicofr.com

SAUVEGARDE et DEVELOPPEMENT

-Génériques

MegaGames. Une foule de cracks, de patchs, de trainers, de cheats, de tutoriaux et d'utilitaires sur toutes les plate-formes: www.megagames.com
GameCopyWorld. Cracks et utilitaires pour faciliter la sauvegarde : www.gamecopyworld.com

-Copie (gravure, modchips, ...)

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

-Spécifiques à certaines machines

Programmer's tools. Tous les outils du programmeur Windows pour le reverse-engeneering : protools.cjb.net
Xbox Scene. Toute l'actualité de l'underground Xbox : www.xbox-scene.com
Xbox-Linux. Installez Linux sur votre Xbox : xbox-linux.sourceforge.net
Spiv's no-mod central. Des tas de patches pour PS2 (malheureusement payant maintenant) : www.nomod-central.com
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
Guide copie Dreamcast. Et en français en plus : membres.lycos.fr/raptor83/dreamcast/copie.htm
Réalisation d'un cable DC->PC : www.ifrance.com/hack128/burn_o.htm

TELECHARGEMENT et ACTU PIRATE

-Web

iSONEWS. La référence de l'actualité pirate : www.izonews.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

-Peer-to-Peer

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

-FTP, News et IRC

SmartFTP. Un client FTP gratuit : www.smartftp.com
newzBin. Traque pour vous les binaries postées sur les News : www.newzbin.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
Classic Trash. Un des sites d'Abandonware les plus respectés : www.classic-trash.com
Home of the Underdogs. Une référence de l'Abandonware que vous ne pouvez pas manquer : www.the-underdogs.org
Oldiesfr.com.. Un site moins fourni, mais en français : www.oldiesfr.com
VDMSound. Pour un son parfait dans les vieux jeux : ntvdm.cjb.net

-Emulation

Zophar's Domain. L'ancêtre est toujours là : www.zophar.net
Emu Unlim. Site très complet dédié à l'émulation : www.emuunlim.com
Linux Emu. L'actualité de l'émulation sous Linux : linuxemu.retrofaction.com
NGEmu. Un bon site d'émulation pour les consoles récentes : www.ngemu.com
Emu-France. Un site français très complet sur toute l'actualité de l'émulation : www.emu-france.com
Toudy. Un site bien sympa en français : www.toudy.com
Emulation64. Toute l'émulation N64 en français : www.emulation64.net
Pdroms. Des tas de roms freeware : www.pdroms.de

JEU ONLINE

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

CHEATS

GameFaqs. Tous les guides et cheats pour tous les jeux : www.gamefaqs.com
Game Software Code Creators Club. Un site de passionnés qui créent eux-mêmes leurs cheats : www.cmgsccc.com
Club Français des Créateurs de Codes Action Replay. N'est plus mis à jour, mais vous pourrez y trouver de l'aide : cfccar.free.fr
The Secrets of Professional GameShark Hacking. Une compilation des meilleurs trucs 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