Bel 3,20 euros, DOM 3,10 euros, CAN 4,25 $ Can

N°10 FÉVRIER-MARS 2005 - SCANDALEUX PIRAT'Z AUGMENTE DE 0,5 €

PIRAT'Z

HACKERS & GAMERS

2,5€

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

Piratez la CIA le jeu ● **Busted!**

Serrés par les keufs ils témoignent

Stégano, Firewalls ● **Vicieux auto-keygen**

Rippez les Webradios en MP3

HDLoader : jeux PS2 sur HD

L 19302 - 16 - F: 2,50 € - RD

Edito

Leet attitude

Plus je lis les autres mags de hacking dans les kioskes, plus je me dis que Pirat'z est quand même le plus l33t! Entre HNM qui se prennent pour des hackers, Zataz, qui eux se prennent pour des journalistes, l'Hackademy qui se croient de la scène ou Hackin9 qui pensent parler français, je me dis que Pirat'z rox pas mal du tout. Nous, au moins, on se prend pour des dieux, mais on a les moyens.

Enfin, on fait semblant, mais on le fait bien. Du moins j'espère. C'est pas facile pour des leet de vous composer des articles newbie de qualité, et qui vous fassent apprendre des trucs au passage. C'est qu'on y met de l'amour. On est pas comme ça, à Pirat'z, on pense qu'il faut tout vous dire ou presque. Ce que l'on garde pour nous, c'est justement ce qui nous permet de hacker la CIA, et de gagner à uplink.

Dans ce numéro, sans cédérom, comme au bon vieux temps, on a tâché de vous gâter, vu qu'on a loupé Noël. Ça commence fort avec les mots de passe Windows. Assez pointu, mais vraiment intéressant, accrochez-vous. Et puis on vous a assuré une petite partie pratique pour peu que vous vous endormiiez. On vous explique aussi plus loin des tas de trucs, comme la stégano, les keygens, les firewalls, tout ça avec des expériences à faire chez vous. À la fin, y a encore plein de bidouilles à faire avec vos console de jeu.

Et si ça vous plait pas, vous n'avez qu'à vous plaindre !

http://piratz.kicks-ass.net

de Bazande

Sommaire

Passwords Windows	p. 3	Bugtraq 2004	p. 20
Intro à la stegano	p. 6	Hackez la CIA	p. 22
Qu'est-ce qu'un Firewall ?	p. 8	Les secrets de la XBOX	p. 24
Auto-Keygen	p. 10	HDLoader pour PS/2	p. 26
Ripper une webradio	p. 12	GameBoy Advanced ++	p. 28
Hack et calculettes	p. 14	Sang d'Encre	p. 29
Busted !	p. 17	Courrier	p. 30

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
Rédacteur en chef assistant : Kanar
Conception Graphique : WEEL
Courrier des lecteurs : Khan
Illustrations : Lechatkitu

Imprimé en CE
ISSN 1638--4458, commission paritaire en cours, dépôt légal à parution,

MPAA veut assécher BitTorrent

Après supmova.org, youceff.com, voilà que LokiTorrent est en danger. Un message sur la page d'accueil du site annonce qu'un procès est officiellement en cours contre ce moteur de recherche. On vous y propose même de participer aux frais d'avocats, estimé à 30.000 $ par mois (pas facile de se défendre contre des monstres qui génèrent des milliards de revenus). De quoi les encourager à résister jusqu'au bout, puisque assez d'argent pour tenir un premier mois a déjà été généreusement rassemblé par la communauté.

On dirait bien que BitTorrent est clairement dans le collimateur de l'industrie cinématographique. À part des taux de transfert largement supérieurs aux autres types de p2p, ce protocole n'est pourtant pas adapté au piratage, puisqu'il est centralisé, peu anonyme, et surtout parce qu'il ne propose pas de fonctions de recherche. C'est justement ce dernier point qui fait la popularité des sites répertoriant les torrents. Il semble que la MPAA n'ait pas négligé l'importance de ce maillon faible.

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.

A L'ASSAUT DES PASS WINDOWS

On vous a déjà dit que la gestion des mots de passe Windows, c'était pas la joie ? Eh bien là, on vous donne l'occasion de savoir pourquoi, et en profondeur. Seulement voilà, faut s'accrocher...

QUE CEUX QUI PRENNENT PEUR TOURNENT LA PAGE, Y A DE LA PRATIQUE !

UN PEU DE THÉORIE...

Windows dispose de plusieurs composants participant à l'identification/authentification.

Le **Winlogon** permet de gérer les ouvertures et fermetures de sessions d'une machine locale et s'occupe aussi de créer l'environnement, c'est-à-dire votre souris, votre clavier, votre écran, vos bureaux. Il est le premier processus lancé, et est lancé à chaque fois qu'un utilisateur appuie physiquement sur le SAS (Security Attention Sequence), qui correspond à l'appui simultané des touches Ctrl-Alt-Del.

L'ARCHITECTURE DE WINLOGON EST GÉRÉE PAR TROIS COMPOSANTS :

- le processus "winlogon.exe" qui ne peut être arrêté,
- une DLL d'identification et d'authentification graphique (GINA, Graphical Identification And Authenticiation),
- et d'autres DLL pour le réseau permettant les connexions avec des réseaux dits non compatibles avec Windows.

Après le SAS entré, notre GINA charge la fenêtre de démarrage que tout le monde connaît, où vous devez entrer votre nom d'utilisateur, votre mot de passe et voir votre domaine. Ensuite vos informations (nom, mot de passe, domaine) sont envoyées par Winlogon au LSA qui va créer un jeton d'accès (expliqué plus bas). Ce jeton d'accès sera utilisé par Winlogon pour créer le shell de l'utilisateur, ou l'environnement si vous préférez (profil, connexion réseau, etc.). À savoir que le SAS par défaut de Winlogon est Ctrl-Alt-Del gérer par "msgina.dll" et qu'il peut être changé. Ce SAS spécifique sera géré par une DLL GINA de remplacement à développer. Vous devrez alors indiquer quelle est cette nouvelle DLL dans la base de registre.

Le **Netlogon** permet, au contraire de Winlogon, de gérer les ouvertures et fermetures de sessions réseaux, par exemple lorsque vous voulez accéder au dossier partagé d'un copain. Ces informations sont ensuite transmises de manière sécurisée par un jeu de Challenge/Response que nous expliquerons un peu plus loin.

Le **LSA** (local security authority) gère et applique les stratégies de sécurité disponibles dans les outils d'administration dans le panneau de configuration. Ce service est géré par le processus nommé "lsass.exe" qui est constamment actif dans le gestionnaire des tâches. Ce service était vulnérable par une faille de sécurité qu'exploitait le virus Sasser.

Le LSA reçoit les informations de Winlogon pour les analyser et intervenir en début de session pour s'assurer si un utilisateur possède la permission d'accéder au système ou non. Pour vérifier cette permission, le LSA contacte le SAM par l'exécution d'une librairie (msv1_0.dll) pour comparer si les informations entrées sont identiques avec celles de la base. Les informations renvoyées par la base sont envoyées à notre librairie qui les renvoie au LSA. En cas de succès d'identification, le LSA crée les jetons d'accès (Security Access Token) contenant beaucoup d'informations comme le SID du compte utilisateur, le SID du groupe auquel appartient l'utilisateur, la liste des droits de l'utilisateur ou du groupe utilisateur, un DACL par défaut, etc.

Le **SAM** (Security Accounts Manager) est le gestionnaire de comptes. Il possède une base de données des comptes utilisateurs autorisés à rentrer sur le système et permet donc au LSA d'authentifier les utilisateurs à sa librairie qui contacte celle-ci.

Lorsqu'un utilisateur veut se connecter en local, la librairie demande au SAM de vérifier que les informations entrées par l'utilisateur sont similaires à celles de sa base pour une authentification avec le service Winlogon.

Dans le cas où la connexion serait sur un domaine, la librairie fait suivre les informations de l'utilisateur vers la base du DC (Domain Controller) pour une authentification avec le service Netlogon.

Le SAM possède une librairie du nom de "samsrv.dll" qui permet de gérer les entrées/sorties de sa base.

Le **SRM** (Security Reference Monitor) est le moniteur de référence de la sécurité. Il intervient pour vérifier les droits d'accès sur les objets et renforce ainsi les audits. On peut distinguer deux types d'objets :

- les objets visibles comme le registre, les fichiers, les répertoires...
- les objets invisibles comme les ports de communication, les processus...

Ainsi, pour vérifier ces contrôles d'accès, le SRM fait une comparaison entre le jeton d'accès créé par le LSA et les permissions définies dans une ACL, la DACL. Nous comptons deux ACL, l'ACL discrétionnaire, **DACL** (Discretionary Access Control List) et l'ACL système, **SACL** (Sytem Access Control List). Le SACL n'a réellement rien à voir avec le contrôle d'accès, nous ne parlerons que de l'ACL discrétionnaire.

La DACL contient des **ACE** (Access Control Entries) supportées par **NTFS** (Windows NT File System) qui permet de spécifier les droits que l'utilisateur ou le groupe possèdent sur un fichier ou un dossier. C'est pour cela que NTFS fait partie de ce système, rappelons-nous les droits NTFS !

LA STRUCTURE DU SAM

Un fichier portant le nom de "sam" contient cette base SAM qui est située dans "%windir%\system32\config" (%windir% fait référence au répertoire de Windows, par exemple c:\Windows) mais ce fichier reste bloqué et inaccessible même aux administrateurs pendant que l'OS est en utilisation. Il existe un autre exemplaire servant de copie de sauvegarde qui est créé lors de l'installation de Windows dans "%windir%\repair" qui n'est accessible qu'aux administrateurs cette fois.

L'ensemble des comptes et des mots de passe sont aussi stockés dans la base de registre (BDR), dans une ruche, qui n'est qu'autre qu'un appel au fichier SAM :
[HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users] (restreint aux comptes qui ne sont pas administrateurs).

Chaque mot de passe subit tragiquement deux gros complexes (tousss...) algorithmes pour garantir une confidentialité, du moins essayer :

L'algorithme **LANMAN** (LanManager ou LM hash) est le type d'empreinte le plus ancien conservé pour des raisons de compatibilité avec les réseaux utilisant le protocole SMB (Windows 95, etc). Le LM hash utilise des mots de passe ayant une longueur maximale de 14 caractères. Chaque mot de passe est complété par des caractères nuls s'il n'atteint pas ces 14 caractères, pour ensuite être divisé en deux groupes de 7 caractères. Chaque minuscule est ensuite mise en majuscule puis ces deux blocs sont cryptés par du DES pour être concaténés et former le LM hash. Les deux groupes de 7 caractères accentuent la faiblesse, étant donné qu'il nous suffira de trouver à chaque fois des mots, mais de 7 lettres seulement.

L'algorithme **NTLM** (NT hash), plus évolué, est quant à lui obtenu en appliquant du MD4 sur le mot de passe chiffré converti en unicode, ce qui forme une empreinte de 16 octets. Le **MD4** (Message Digest 4) est rapide, mais ça peut aussi se casser assez facilement (MD5 n'a pas été conçu pour rien, et encore). Mais le problème, c'est que l'on trouvera le plus souvent le hash LM avec le hash NTLM. Donc, si on cracke le premier, ce qui est encore plus facile, on aura aussi cassé le hash NTLM, pour autant que l'on teste toutes les combinaisons de majuscules et minuscules, qui ont une importance cette fois.

Si votre réseau ne comporte pas de Windows inférieur à NT4, vous devriez interdire le LM.

CONCLUSION

Maintenant que nous vous avons montré comment fonctionnait l'authentification Windows dans son ensemble, vous êtes capables de comprendre ce que nous allons vous montrer dans cette partie pratique, et serez en mesure de capturer vos hashes avec Pwdump et de vérifier la solidité de vos mots de passes avec LC5 ou des Rainbow Tables.

XeLoRy

PASSWORDS WINDOWS

Vous avez craqué ? Je veux dire : zappé la page précédente ? Voici une nouvelle chance de comprendre les faiblesses de vos mots de passe, par la pratique cette fois.

PWDUMP, LE DUMPER DE SAM

Pwdump a déjà un premier avantage : il est libre et gratuit, sous licence GPL !

Nous rencontrons plusieurs versions, pwdump, pwdump2 de Todd Sabin et pwdump3 de Jeremy Allison. Pwdump2 agit localement alors que pwdump3 peut agir à distance. Pwdump est disponible dans chaque distribution SAMBA ou partout sur le Net. Voici tout de même un lien pour les plus flemmards d'entre vous : http://packetstorm.linuxsecurity.com/Crackers/NT/. Comme expliqué dans la partie théorie, le fichier SAM n'est pas facilement accessible. C'est à cela que pwdump servira : nous simplifier la vie.

Une des rares choses disponibles et voulues sur Internet, c'est de savoir comment fonctionne la chose. Encore un peu de théorie ; patience est la route vers la gloire.

Pwdump est composé d'une application (pwdump2.exe) et d'une DLL (samdump.dll)

Un pipe sera établit entre notre processus (pwdump2.exe) et lsass.exe grâce à samsrv.dll, la librairie qui gère les entrées/sorties de la base SAM. Notre pwdump2.exe obligera lsass.exe à charger samdump.dll pour exécuter son code. La méthode est appelée "une injection de DLL". Notre librairie utilise la même API interne que celle utilisé par msv1_0.dll, la DLL qui permet d'accéder aux mots de passe et bénéficiera ainsi des droits d'utilisateur SYSTEM. Pwdump2.exe trouvera de façon automatique le PID (processus identification) de lsass.exe et ainsi permettra de faire un dump hexadécimal du SAM.

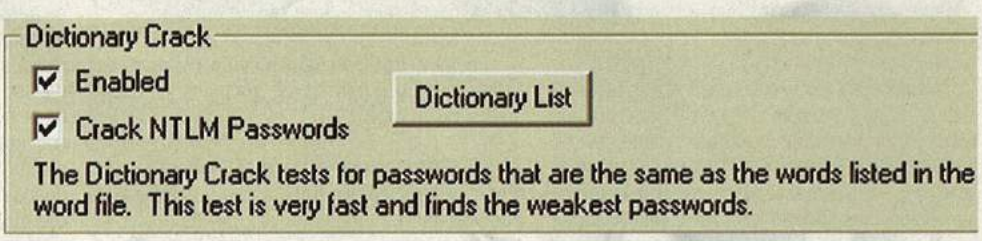
Pour commencer, lancez l'interpréteur de commande (démarrer>exécuter>cmd), rendez-vous dans le répertoire où se trouvent vos deux fichiers (utilisez pour cela la commande cd suivie du chemin du répertoire, par exemple "cd c:\hacking\pwdump"), puis tapez simplement : "pwdump2.exe". Validez par entrée. Vous devriez avoir un résultat à l'écran, mais le plus pratique serait d'enregistrer le tout dans un document texte. Pour cela, tapez : "pwdump2.exe>sam.txt". Ouvrez votre fichier texte sam.txt get. Vous devriez avoir quelque chose sous la forme "NOM:RID:HASHLM:HASHNT", comme ci-dessous:

```
Administrator:500:89b61c90c8d94de8aad3b435b51404ee:51cecb3620aa7392\
67cc971a289a3659:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d\
7e0c089c0:::
HelpAssistant:1000:67267658878d20a32e50e24c3bb7a4e5:4bb0a3e4f2f3b2e\
a665f4a06849134ce:::
nghw:1003:89b61c90c8d94de8aad3b435b51404ee:51cecb3620aa739267cc97\
1a289a3659:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0bd8f06a8d\
658646b64a3af5838a54d4:::
```

Et voilà ! Vous êtes maintenant en possession des mots de passe cryptés, il ne reste plus qu'à tester leur solidité avec LC5.

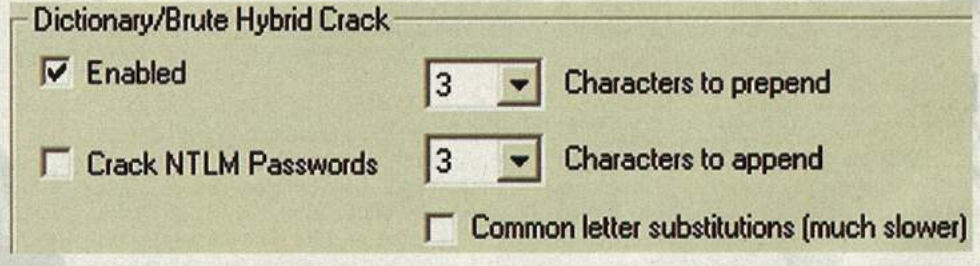
LC5

L0phtCrack est un utilitaire permettant de tester l'efficacité des mots de passe en utilisant des méthodes d'audit. Beaucoup d'entreprises utilisent chaque jour LC pour vérifier la présence de mots de passe faibles. On peut distinguer plusieurs possibilités d'audit dans les préférences (File puis Preferences...) avec ce fameux logiciel :



La méthode par **dictionnaire** consiste à essayer tous les mots disponibles dans une liste. Vous devrez ajouter vos dictionnaires à l'aide du bouton "Dictionnary List".

Cette technique est assez intelligente : elle permet de s'orienter dans un domaine bien précis. Par exemple,



en sachant que l'utilisateur est un fan de cinéma, il pourrait ainsi se procurer une liste des noms des acteurs. C'est ce que ferait un pirate, et ce que devrait faire l'administrateur pour tester les passes de ses utilisateurs.

PAR LA PRATIQUE

La méthode dite **Hybride** consiste à ajouter un ou plusieurs caractères au début ou/et à la fin de chaque mot contenu dans le dictionnaire. Cette stratégie permet rapidement de repérer les mots de passe assez futiles comme "bizou69" ou encore "!=bateau".

La méthode par **Brute Force brute** consiste à essayer toutes les possibilités de caractères pour parvenir à trouver le mot de passe. Cette technique peut être longue, voire très fatigante.

La nouvelle version de LC inclut une nouvelle méthode appelée **Precomputed** que je juge la plus élaborée. Nous détaillerons cette méthode dans un prochain numéro (les fameuses Rainbow Tables).

Retrieve from the local machine

1 Pulls encrypted passwords from the local machine registry. Administrator access is required.

Bien que vous ayez aperçu un résumé des méthodes de LC, vous ne connaissez pas encore ce dont ce dernier est capable ! Lors de la première ouverture de LC, un wizard (assistant) démarre et vous propose quatre méthodes pour importer les mots de passe :

Retrieve from a remote machine

2 Retrieve encrypted passwords from a remote machine on your domain. Administrator access is required.

- La première consister à importer les mdp cryptés par la BDR de la machine locale où un accès administrateur est requis. (1)
- La deuxième méthode consiste à importer les mdp cryptés, toujours par la BDR, mais cette fois ci d'une machine distante Windows. LC5 permet maintenant d'importer des fichiers shadow ! L'accès administrateur est encore requis. (2)
- La méthode suivante est la récupération à partir d'un fichier SAM autre que celui utilisé actuellement par Windows, celui de la sauvegarde système par exemple (%windir%\repair\) ou encore un fichier récupéré grâce à NTFSDOS (utilitaire très simple que je vous laisse découvrir par vous-même), ou un autre système ne protégeant pas le SAM comme Linux. (3)

Retrieve from NT 4.0 emergency repair disk

3 Emergency repair disks and backup tapes made from Windows NT 4.0 contain a file called 'sam' o 'sam._' that contains encrypted passwords.

Retrieve by sniffing the local network

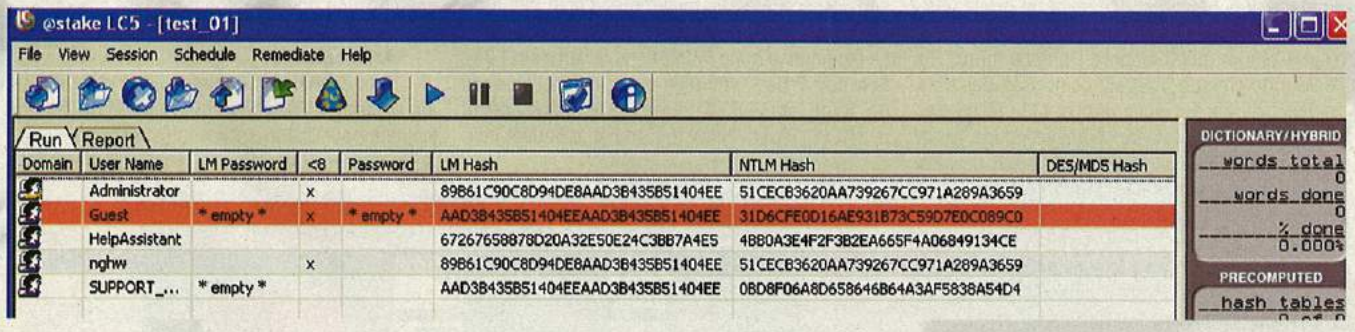
4 Sniffing captures encrypted hashes in transit over your network. Logins, file sharing and print sharing all use network authentication that can be captured

- La dernière méthode permet de mettre en place un sniffer qui capturera les hashes cryptés qui transitent sur le réseau local sur les services d'authentification réseau comme les connexions réseaux SMB, les fichiers et imprimantes partagés. (4)

Vous pouvez avoir le choix de passer avec l'assistant ou alors de faire les importations vous-même. Lancez une nouvelle session en cliquant sur :

Ensuite, dirigez-vous dans l'onglet "Session" puis cliquez sur "Import...". Une fenêtre s'ouvre et vous ne devriez pas être surpris par les options étant donné que ce sont pratiquement les mêmes que celles proposées dans l'assistant. Vous pouvez tout de même apercevoir deux nouvelles options : "From LC4 file" et "From PWDUMP file". Il s'agit d'une simple importation des sauvegardes de session de LC4 et fichiers PWDUMP dont nous avons fait la démonstration.

Vous l'aurez compris, nous allons maintenant importer notre fichier PWDUMP.



Voici le résultat obtenu pour mon fichier personnel :

LC5 a bien entendu pensé aux outils pratiques que vous découvrirez par vous même, tels que la sauvegarde de session en fichier *.lcs, l'exportation des mots de passe et de sessions et la planification d'audit qui utilise le planificateur de tâche de Windows. Maintenant, passons à cette nouvelle méthode dite Rainbow Crack.

CONCLUSION

Vous avez sans doute pu voir à quel point le déchiffrage de l'un de vos comptes est rapide. Restez prudents, définissez des mots de passe solides. Des majuscules, des minuscules, des chiffres, des caractères : n'hésitez pas à faire compliqué. Et surtout, testez-les !

Nous découvrirons dans le numéro suivant "RainbowCrack", des tables précompilées qui permettent le déchiffrage d'une hash en quelques secondes ainsi que d'autres outils qui vous permettrons de tester la fiabilité de vos systèmes. À venir par logique, nous verrons un article sur la manière de sécuriser son Windows.

XeLoRy

Le futur appartient à ceux qui croient à la beauté de leurs rêves

L'ART DE DISSIMULER

La stéganographie est l'art de dissimuler des données (par exemple du texte) dans d'autres données servant de support (une image, un mp3), sans trop changer l'apparence de ce support pour que cela passe inaperçu - sauf évidemment aux yeux du destinataire, qui connaît le procédé.

Le point fort de la stégano est très simple à trouver : un support apparemment anodin passera bien plus inaperçu qu'un fichier explicitement crypté. Je vous laisse imaginer l'ampleur du travail si l'on voulait vérifier chaque fichier de votre système (y compris les gros dossiers d'images planqués vous savez où) à la recherche de texte caché. En plus, il n'est pas toujours facile de déterminer si un fichier contient des données stéganographiées. Et de toutes façons, rien ne vous empêche de crypter les données avant de les cacher, pour encore plus de sécurité ;-)

Les heureux possesseurs du *Manuel des castors juniors* ont déjà vu l'exemple de l'encre sympathique : du jus de citron qui devient visible lorsqu'il est à proximité d'une source de chaleur. On peut y voir une première méthode de stéganographie. Mais rassurez-vous, ce procédé archaïque est depuis longtemps remplacé par des méthodes bien plus efficaces, notamment depuis l'avènement de l'informatique. L'exemple de stéganographie moderne le plus courant est la dissimulation de texte dans une image : c'est celui que nous allons étudier aujourd'hui.

POINT PAR POINT

Avant d'entamer cette étude théorique, attardons-nous un peu sur les caractéristiques d'une image au format le plus simple : bmp. Pour un ordinateur, une image est une suite de pixels (élément de base d'une image ou d'un écran, c'est-à-dire un point coloré). Dans ce format, la couleur de chaque pixel est composée des trois couleurs de base : rouge, vert et bleu (à ne pas confondre avec les couleurs primaires rouge, jaune et bleu): on dit qu'il utilise le codage RVB (je vous laisse deviner d'où vient le nom du codage ;-)

Au niveau du stockage, chaque pixel est donc codé par 3 nombres correspondants à l'intensité de chaque couleur dans cet ordre : rouge, vert, bleu. Certains formats permettent de spécifier une troisième composante : la transparence. En imprimerie, on a aussi une composante encre noire.

Un peu de mathématiques maintenant mais rien de bien compliqué :

Un nombre hexadécimal est un nombre en base 16. Je m'explique. Quand vous comptez normalement, vous comptez de 0 jusqu'à 9, puis vous ajoutez 1 devant et vous recommencez à 0 derrière : vous êtes alors en base 10 (c'est un nombre décimal), c'est-à-dire que vous comptez avec 10 "signes" : 0 à 9. En hexadécimal, les nombres sont en base 16 : on utilise donc combien de signe ?

Si vous avez répondu 16, vous pouvez continuer, sinon plongez-vous la tête dans un seau d'eau froide et recommencez le paragraphe. En effet, en plus des chiffres de 0 à 9, on utilise les lettres A à F de notre alphabet, ce qui fait 16 signes différents. Donc, si vous avez suivi :

A vaut 10 en décimal, B vaut 11, etc. jusqu'à F qui vaut 15 (toujours en décimal).

On compte ainsi : 0, 1... 9, A, B, C, D, E, F, 10, 11... 19, 1A, 1B... 1F, 20, etc.

Rassurez-vous, vous n'êtes pas obligé de faire ces calculs à la main si vous n'êtes pas habitué à l'hexa(décimal) : la calculatrice de Windows (Démarrer > Exécuter > calc) le fait très bien (en affichage scientifique mode héxa).

Bon, c'est bien beau tout ça, mais quel est le rapport avec la choucroute ? Le voici : en bmp, chaque composante de couleur est un nombre compris entre 0 et 255, soit entre 0 et FF en hexa (essayez donc sur la calculette). Une couleur peut donc être codée par un suite de trois nombres (chacun compris entre 0 et FF), lesquels correspondent aux trois composantes rouge, vert et bleu (dans cet ordre). Ce code, appelé hexadécimal (le même qui est utilisé pour coder les couleurs dans les pages web), ressemble donc à ceci : `#E322F6`.

On peut le décomposer en trois nombres codant le rouge, le vert et le bleu (dans cet ordre) sans espace. Ainsi, le rouge "pur" s'écrit `#FF0000` pour "`255 (FF)` de rouge, 0 de vert et 0 de bleu". Le bleu donne donc `#0000FF` et le vert `#00FF00`. Et le noir ? Ben `#000000` puisque c'est l'absence de toute couleur. À l'inverse, le blanc s'écrit `#FFFFFF`. Pour vérifier tout ça, vous pouvez utiliser Paint Shop Pro ou Gimp (disponibles sur telecharger.com ou gimp.org), ou tout autre éditeur d'image assez complet.

Sous Paint Shop Pro, lorsque vous double-cliquez sur l'outil de choix des couleurs, vous avez alors une boîte de dialogue avec un champs "Code HTML" (voir capture).

NUANCES INVISIBLES

Nous entrons maintenant dans le vif du sujet. Puisque vous avez ouvert Paint Shop Pro, entrez ce premier code dans "Code HTML" : `#F545C6` (vous devez obtenir un rose-mauve) et validez. Puis cliquez à nouveau sur le même rectangle de couleur, et remplacez le deuxième chiffre de chaque composante par 0 : `#F040C0` et comparez la couleur en cours avec la couleur précédente (à droite, voir capture) : quasiment pas de changement ! Sans fermer, entrez maintenant le même code en remplaçant les 0 par des F : `#FF4FCF`. Là aussi, le changement est quasiment invisible à l'œil nu. Vous venez d'appliquer, sans le savoir, un principe de stéganographie.

Explications :

Entre `FØ (240)` et `FF (255)`, il n'y a que 15 (si, si) ce qui, sur une échelle de 255, n'est pas énorme (6 %). Avec le mélange des trois composantes, même l'écart maximum causé par la modification du dernier chiffre passe inaperçu.

Application :

Pour cacher des données dans cette image, on va donc utiliser le dernier chiffre de chaque couleur pour chaque pixel.

Code couleur HTML

LES DONNEES

On peut donc avec cette méthode stocker soit trois nombres (entre 0 et 15) pour chaque pixel, sachant qu'une image bmp est composée de millions de pixels, ça nous laisse un bon espace exploitable !

CODAGE

Supposons maintenant que nous décidions d'utiliser un alphabet des 256 caractères (espace, a-z, A-Z, 0-9, accents et quelques caractères spéciaux), chaque caractère correspond alors à un nombre compris entre 0 et 255. Vous voyez où je veux en venir : sur chaque composante de l'image, on va remplacer le dernier chiffre par l'un des chiffres de notre alphabet. Sachant qu'il faut deux chiffres hexadécimaux pour faire le nombre de notre caractère, il faudra donc regrouper deux par deux les derniers chiffres de composantes lors de l'extraction.

Action :

Prenons l'alphabet suivant (0 sera le code pour l'espace) :

Décimal	0	1	2	...	25	26	27	...	51	52	...	62	63	...	255
Hexa	00	01	02	...	19	1A	1B	...	33	34	...	3E	3F	...	FF
Caractère	espace	a	b	...	z	A	B	...	Z	0	...	9	Autres ...		

On réserve un nombre (par exemple 255) pour indiquer la fin du message.

Le message à cacher :

Caractère	C	e	c	i		e	s	t		1	t	e	s	t
Décimal	28	5	3	9	0	5	etc...							
Hexa	1C	05	03	09	00	05	etc...							

Ce qui nous donne en hexa :
1C 05 03 09 00 05

Notre image commence par quatre pixels noirs :
#FFFFFF #FFFFFF #FFFFFF #FFFFFF

On la modifie comme suit :
#F1FCF0 #F5F0F3 #F0F9F0 #F0F0F5
et ainsi de suite...

On obtient une nouvelle image, avec le texte caché à l'intérieur.

Pour extraire ce texte, on procède exactement de la manière inverse :
#F1FCF0 #F5F0F3 #F0F9F0 #F0F0F5 ...

Hexa	1C	05	03	09	00	05	etc...
Décimal	28	5	3	9	0	5	etc...
Caractère	C	e	c	i		e	etc...

QUELLES IMAGES CHOISIR ?

L'idéal est une image qui possède beaucoup de couleurs différentes, comme une photo. En effet, si l'image est trop unie (exactement la même couleur sur beaucoup de pixels), on risque de voir les légères variations apparaître, lesquelles sont invisibles sur une photo. Préférez également les photos personnelles à celles trouvées sur Internet, car ainsi il est impossible de comparer la photo modifiée à l'originale, ce qui pourrait éveiller des soupçons si elle tombait dans de mauvaises mains. Dernier critère : la taille. En effet, la technique ci-dessus exige que la taille de l'image soit suffisante pour stocker l'intégralité du message.

Je vous conseille de vous faire une réserve personnelle d'une dizaine d'images afin de ne pas faire circuler toujours la même, ce qui pourrait également soulever des questions.

CONCLUSION

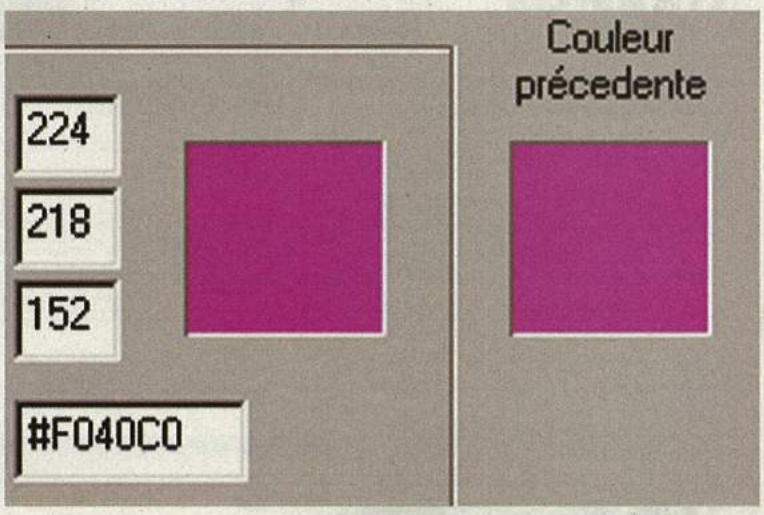
Nous avons donc vu comment cacher du texte dans une image. Sachez cependant que cette technique n'est pas la seule dans le domaine de la stéganographie. Il en existe d'autres, notamment celle du Slack Space, qui permet de cacher des données dans les espaces non-utilisés par un fichier (quelque soit son type).

LOGICIELS

La manipulation ci-dessus est bien évidemment destinée à vous faire comprendre une technique de stéganographie, et non à être employée pour cacher effectivement vos données, car en plus d'être très basique (quelqu'un qui la connaît trouvera facilement le message caché), elle est manuelle, donc longue et fastidieuse.
Il existe pas mal de logiciels gratuits qui se feront un plaisir de cacher vos données dans tous types fichiers, et pas seulement des images. Je vous conseille l'excellent Steganozorus (http://thomasnerrant.com/, par l'auteur de Cryptozor) ou encore Secure Engine (http://securengine.isecurelabs.com/).

Notez également que, si dans l'exemple ci-dessus on a inséré du texte, il est possible de cacher d'autres type de données.

Eks



Quelle est la différence ?

DIS, C'EST QUOI

Si vous pensez qu'un firewall peut empêcher un pirate d'entrer sur votre ordinateur, vous devriez lire ce qui suit. On vous y explique comment ça marche et à quoi ça sert, en réalité.

QU'EST CE QU'UN FIREWALL ?

Vous avez sûrement entendu parler sur Internet de pare-feu, de coupe-feu ou de "firewall" (du même nom que les portes coupe-feu en anglais). Il s'agit d'une application ou d'une machine qui se place à une embouchure d'un réseau, et qui analyse systématiquement les connexions entrantes et sortantes, et les données qui y transitent. Il vous assure une certaine protection en analysant la couche réseau, la couche transport, ou même la couche application pour les firewalls personnels.

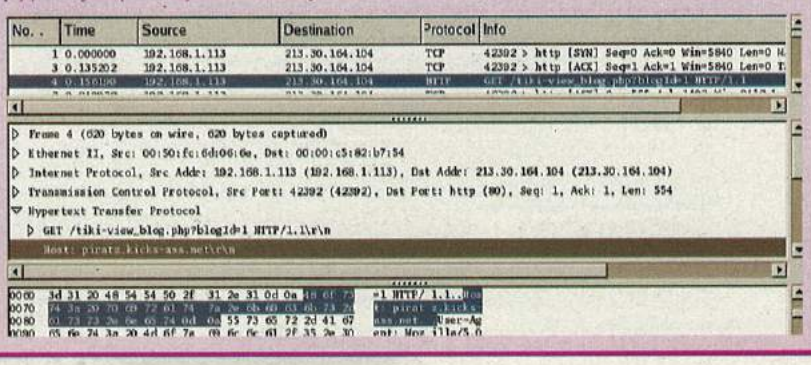
TCP/IP

Les données numériques transmises électroniquement entre deux points sont codées selon un ou plusieurs protocoles, sur plusieurs couches. En général, on les segmente en paquets de données, auxquels on ajoute des méta-informations, qui constituent une en-tête. Lorsque le média de communication est commun à plus de deux entités, il est par exemple nécessaire de spécifier, en plus des données, qui doit recevoir (destinataire), et qui envoie (émetteur). Sur un réseau ethernet, c'est le rôle des adresses mac, qui apparaissent dans l'en-tête. Sur le Net, puisque les paquets sont distribués dans tous les sens par les FAI et les gros routeurs nationaux et continentaux,on spécifie les adresses IP.
Ces méta-informations sont hiérarchisées selon les différentes couches de transport. En effet, votre carte réseau n'a pas besoin de savoir que vous voulez vous connecter à un service web pour transmettre correctement le paquet au routeur Internet. On a donc une encapsulation, que l'on peut représenter comme ceci :

```
Eth  : [MAC source/dest,..] [contenu.....]
IP   :                      [IP src/dest,..]  [contenu.....]
TCP  :                                        [ports,...] [contenu.....]
```

On voit que l'on peut décomposer un paquet ethernet en une en-tête (en bleu) plus un paquet IP, qui lui-même contient une en-tête et un paquet TCP.
Les en-têtes contiennent beaucoup d'informations importantes. Par exemple, des flags de l'en-tête TCP permettent de négocier des connexions (le fameux syn/ack).

Une bonne manière de comprendre tout cela est de visualiser les différents protocoles à l'aide d'un analyseur, par exemple Analyzer out Ethereal (voir capture).
http://www.ethereal.com/
http://www.ethereal.com/
http://analyzer.polito.it/



Certains pare-feu permettent aussi d'autoriser la communication d'un processus à une date donnée, pendant un certain laps de temps.

LE FILTRAGE DE PAQUETS :

Allez, c'est aujourd'hui que vous devenez un vrai hacker ! Nous allons parler des entêtes TCP/IP ;-)

Un pare-feu fonctionne sur l'analyse d'en-têtes de paquets TCP/IP (voir encadré) : c'est-à-dire que lorsqu'un paquet entre ou sort d'un réseau, son en-tête est vérifiée. Mais de quoi une entête est-elle constituée ?

- de l'adresse IP de l'émetteur du paquet,
- de l'adresse IP du récepteur du paquet,
- du type de paquet (TCP en mode connecté, UDP en mode non-connecté),
- et du numéro de port de service utilisé par le paquet.

Une adresse IP permet d'identifier la machine qui émet et la machine qui reçoit les paquets. Elle est de la forme suivante : xxx.xxx.xxx.xxx où chaque xxx est un nombre de 0 à 255, et spécifique à chaque PC relié à Internet : à chaque fois que vous mettez les pieds sur le Net, une adresse de ce type vous est attribuée par votre fournisseur d'accès et permet de vous identifier sur le réseau.

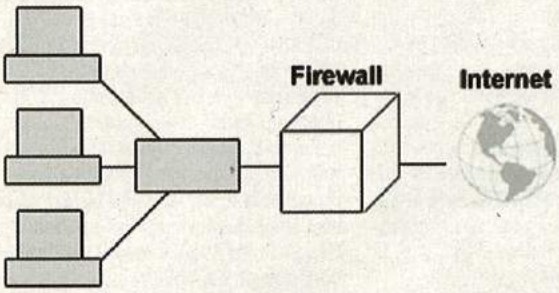
Le type, puis le numéro de port nous donnent des informations sur le service utilisé. Par exemple le port 80 est utilisé par les serveurs internet, le port 21 utilisé pour une connexion FTP, etc.

Un firewall vous permet donc de dire quels paquets vous désirez laisser passer. Vous voudrez par exemple interdire tous les paquets entrants sur votre réseau avec 80 comme port destination, parce que votre serveur web est privé (réservé à votre LAN), ou interdire les ports 135-139 en entrée, pour éviter le partage de fichier Windows avec le reste du monde, ou encore interdire le port 1863 en sortie, pour empêcher votre petite sœur de se connecter à MSN. Plus futé, on peut bloquer d'office les ports 1234, 12345, 31337 et autres, qui sont réputés pour être utilisés par des backdoors et autres trojans. Si vous êtes un utilisateur qui surf simplement sur le Net sans faire de programmation ou quoi que ce soit, il est d'ailleurs préférable pour plus de sécurité de bloquer tous les ports en entrée. De cette façon, même si vous lancez par mégarde un Cheval de Troie, le pirate aura plus de peine à se connecter sur votre machine depuis le Net.

UN FIREWALL ?

LA PLACE D'UN PARE-FEU

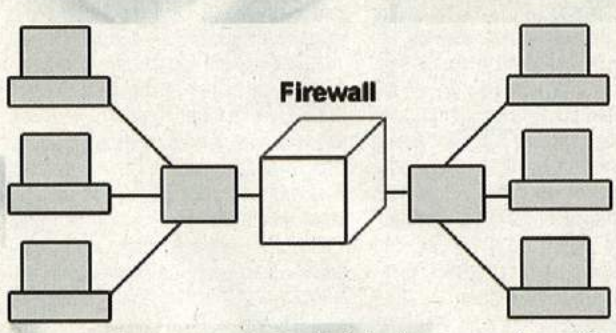
Entre le réseau et Internet



Là, le pare-feu est une machine placée physiquement entre le réseau local et Internet. Je précise aussi qu'un pare-feu peut être incorporé dans un routeur.

Cet emplacement permet d'accroître globalement la sécurité des machines, puisqu'on peut surveiller tout le trafic, et supprimer *a priori* tout ce qui est dangereux. Il y a cependant toujours des moyens de passer outre le filtrage.

D'un réseau à un autre réseau



Le pare-feu est encore un matériel physique car il n'est pas directement installé sur un poste du réseau.

Dans cette architecture, il gère les entrées et les sorties des deux réseaux. Ici les réseaux ne sont pas forcément soumis directement aux dangers d'Internet.

On choisit ce genre d'architecture pour cloisonner les parties d'un réseau qui sont plus sensibles que d'autres. On peut avoir d'un côté les postes des employés d'une entreprise et de l'autre les serveurs de fichiers, de backups, etc. Avec un tel firewall, on peut faire en sorte que seuls les postes qui en en besoin puissent se connecter à certains serveurs (pour des questions de confidentialité, par exemple). Du coup, une poste utilisateur compromis par un trojan, par exemple, ne pourra pas directement servir de tremplin à un pirate qui viserait un serveur interne particulier.

Le firewall personnel

Le firewall personnel est un programme directement installé sur un poste. En plus de contrôler le trafic réseau, il peut surveiller les applications qui le produisent. On peut par exemple interdire toutes les connexions vers l'extérieur, sauf celles qui viennent de Mozilla (seulement les ports 80 et 443, plus 25 et 110 pour le mail).

Les avantages d'un firewall personnel :

- il est facile à configurer,
- il peut détecter des backdoors qui passeraient inaperçues sur le réseau (connect back sur le port 80),
- on peut en trouver des libres et gratuits sur Internet.

Les inconvénients :

- c'est beaucoup plus facile à pirater pour un hacker, car une fois qu'il a accès à votre ordinateur, il peut sans aucun problème le désactiver. Il est beaucoup plus difficile de désactiver un firewall physique (pas de contrôle à distance),
- étant donné que c'est un logiciel, il peut éventuellement ralentir votre PC.

CONCLUSION

Je tiens à préciser que vous ne serez jamais hors de danger à 100 %, même si vous avez un pare-feu qui est bien configuré. Il y aura toujours une micro-faille quelque part, petite mais dangereuse.

N'oubliez surtout pas de fermer les applications inutiles qui utilisent Internet, pour ne pas avoir de port ouvert sans que ce soit nécessaire sur votre machine et ainsi éviter les prises de risque superflues.

Si vous avez compris cet article, vous savez désormais comment marche un pare-feu, mais pas comment l'utiliser. Eh oui, il y a des connaissances à acquérir tout seul ! Je peux vous conseiller Google, vous y trouverez facilement des tutoriaux expliquant comment configurer votre firewall préféré.

Voilà, j'espère que j'ai été suffisamment clair et explicite.

Bonne lecture pour les autres articles et continuez à acheter Pirat'z ;-)

xpdeath

LOGICIELS

Voici une liste non exhaustive de firewalls personnels fonctionnant sous Windows :

Gratuits :
- **Windows XP (firewall intégré, activé avec le SP2)**
- **Agniyum Outpost Firewall**
- **eSafe Desktop**
- **Kerio Personal Firewall**
- **Look'n'Stop**
- **Norton Personnal Firewall**
- **Sygate Personal Firewall**
- **Zone Alarm**

Payants :
- **Norton Antivirus 2004 (il y a un pare-feu incorporé)**
- **Zone Alarm version pro**
- **Black Ice Defender**
- **Tiny Personnal Firewall**

Le noyau Linux intègre bien sûr des mécanismes de filtrage puissants (Netfilter), qui sont pilotables en ligne de commande (iptables), ou avec de nombreuses interfaces graphiques (shorewall, guarddog, etc.). Même pour un réseau personnel, c'est une très bonne idée de recycler un vieux PC (genre 486) pour en faire un firewall/routeur.

REVERSE E
AUTO-KEYG

PARTAGEZ C'EST GAGNÉ !

Dans la mentalité judéo-chrétienne, partager est une bonne chose, si vous ne le faites pas, vous irez en enfer ! Et Skype technologies nous le rappelle. Il s'agit d'un éditeur de téléphonie par Internet qui permet aux utilisateurs de partager des documents entre eux (toutefois, rien à voir avec le P2P), et plus ils partagent, moins ils paient. Ceux qui partagent peuvent utiliser ce service gratuitement. Cette campagne de publicité annonce également le début de la collaboration entre Skype technologies et KaZaa, où l'on peut y voir les pubs.

BIENTÔT UN WINRAR UPDATE ?

Parmi tous les logiciels de compression / décompression de fichiers, WinRAR est sans doute un des meilleurs (si ce n'est le meilleur). Parce que bon, WinZIP, c'est sympa 5 minutes, mais quand il s'agit d'avoir un bon taux de compression, ou de décompresser une release récemment téléchargée, on sait bien que ça ne vaut pas de la m****. Mais souvent, parce que le format de compression n'évolue de toute manière que très peu, on ne pense pas à mettre à jour un tel logiciel. Grave erreur ! En effet, une faille et voilà votre ordinateur une cible toute désignée pour vos soi-disant amis lecteurs de Pirat'z... ainsi, un chercheur en sécurité vient de découvrir dans WinRAR une faille permettant d'exécuter du code arbitraire, grâce à un buffer overflow. Cette faille est reliée à une mauvaise gestion du nom des fichiers effacés dans une archive, et il faut donc amener l'utilisateur à effacer un fichier pour l'exploiter. En tout cas, si comme moi vous utilisiez toujours WinRAR 3.0 depuis 2 ans, passez dès maintenant à la 3.42 pour éviter les ennuis.

C'est facile de télécharger un keygen sur le Net. Mais c'est en revanche beaucoup plus intéressant à se demander comment ça marche, rien que pour le fun, et pour ce que ça apprend en matière d'assembleur et de reversing. C'est le but de cet article.

Dans mes précédents articles, on a vu comment les crackers procèdent pour supprimer une protection dans un logiciel, ainsi que pour retrouver un mot de passe. Passons à des choses plus concrètes, plus proches de la réalité. Certains logiciels possèdent une protection par nom et serial. C'est à dire qu'ils vous demandent d'entrer un nom, puis un serial (numéro de série) et vérifient la cohérence. Généralement, le serial est généré en fonction du nom entré, ce qui complique la tâche du cracker car il n'y a aucun mot de passe stocké dans le programme. Ce genre de protection peut être contourné de deux manières : soit on s'arrange pour que le programme accepte tous les couples nom/serial, soit on fait en sorte d'obtenir un couple nom/serial valide.

VOUS AVEZ DIT KEYGENNING ?

La première méthode peut sembler la plus simple, mais se révèle en fait assez complexe : même si on autorise tous les couples nom/serial, il y a toujours un risque qu'une procédure de vérification nous ait échappée. Et donc que le couple nom/serial ne soit plus validé. En pratique, cela se traduit par une modification du programme en deux points : lors de l'entrée du couple nom/serial et lors de la vérification au du démarrage du programme, si vérification il y a. Nous allons nous orienter vers la deuxième méthode. Celle-ci est plus simple, car une fois un couple nom/serial trouvé, il suffit juste de valider et il n'y a aucune modification à apporter au logiciel. La méthode consistant à trouver un couple nom/serial valide est ce qu'on appelle le keygenning. Le principe est simple : si un programme génère un serial à partir d'un nom, il possède obligatoirement la fonction de génération. Il suffit donc d'identifier cette fonction de génération de serial, de l'extraire du programme pour ensuite l'implémenter dans un petit programme, appelé keygen pour l'occasion, qui donnera le serial en fonction du nom entré. Vous grimacez? Ne vous affolez pas, nous allons utiliser un dérivé du keygenning, j'ai nommé l'auto-keygenning.

Le principe de l'auto-keygenning est simple : sachant que le programme va comparer le serial entré au bon serial généré à partir du nom entré, et ensuite afficher un message de réussite ou d'échec, il y a sûrement moyen de le forcer à afficher le bon serial. Cela nécessitera juste une petite modification du programme, qui nous donnera de lui-même le bon serial pour le nom entré. En gros, on aura transformé ce programme en son propre keygen, d'où le nom d'auto-keygenning.

Comme je ne conçois pas un bon article de reverse engineering sans exemple concret d'application, je vous ai concocté un petit programme qu'il va nous falloir auto-keygenner.

REPÉRAGES

La première chose à faire est de lancer le programme. Entrez " toto " comme nom, puis " titi " comme serial. Le programme affiche une boîte de message contenant le texte " Baaaaaaad password !! ". Un bon point pour nous, ce texte apparaîtra dans les références de chaînes de caractères. On ouvre donc le programme avec OllyDbg comme vous l'avez appris donc le précédent Pirat'z et l'on clique droit sur le code ASM. On choisit " Search for ", puis " All referenced text strings ". On double clique ensuite sur la chaîne " Baaaaaaad password !! " que l'on aperçoit à l'écran, pour retomber à l'endroit indiqué dans la capture 1.

```
004014AF | . 83C4 10      | ADD ESP,10
004014B2 | . 83EC 04      | SUB ESP,4
004014B5 | . 83EC 08      | SUB ESP,8
004014B8 | . 68 20504000  | PUSH KEYGENPI.00405020
004014BD | . E8 9E180000  | CALL <JMP.&msvcrt.strlen>
004014C2 | . 83C4 0C      | ADD ESP,0C
004014C5 | . 50           | PUSH EAX
004014C6 | . 8D85 F8FDFFFF| LEA EAX,DWORD PTR SS:[EBP-208]
004014CC | . 50           | PUSH EAX
004014CD | . 68 20504000  | PUSH KEYGENPI.00405020
004014D2 | . E8 79180000  | CALL <JMP.&msvcrt.strncmp>
004014D7 | . 83C4 10      | ADD ESP,10
004014DA | . 85C0         | TEST EAX,EAX
004014DC | .v75 15        | JNZ SHORT KEYGENPI.004014F3
004014DE | . 6A 00        | PUSH 0
004014E0 | . 68 BF134000  | PUSH KEYGENPI.0040138F
004014E5 | . 68 D1134000  | PUSH KEYGENPI.004013D1
004014EA | . 6A 00        | PUSH 0
004014EC | . E8 2F190000  | CALL <JMP.&USER32.MessageBoxA>
004014F1 | .vEB 45        | JMP SHORT KEYGENPI.00401538
004014F3 | > 6A 00        | PUSH 0
004014F5 | . 68 DD134000  | PUSH KEYGENPI.004013DD
004014FA | . 68 F5134000  | PUSH KEYGENPI.004013F5
004014FF | . 6A 00        | PUSH 0
00401501 | . E8 1A190000  | CALL <JMP.&USER32.MessageBoxA>
00401506 | .vEB 30        | JMP SHORT KEYGENPI.00401538
```

```
s = ""
strlen
maxlen
s2
s1 = ""
strncmp
Style = MB_OK|MB_APPLMODAL
Title = "congratulations !"
Text = "Well done !"
hOwner = NULL
MessageBoxA
Style = MB_OK|MB_APPLMODAL
Title = "Very bad bad things ..."
Text = "Baaaaaad password !!"
hOwner = NULL
MessageBoxA
```

1

Avant de continuer, petite analyse de la situation. On remarque tout d'abord une fonction intéressante, à savoir " strncmp ". Elle compare deux chaînes de caractères passées en argument. On peut aussi apercevoir un JNZ 004014F3, qui n'est rien d'autre qu'un saut vers l'affichage de la boîte de message (MessageBox) du mauvais serial. La commande JNZ (Jump if Non Zero) indique au programme de sauter en 004014F3 si le résultat de la fonction " strncmp " est différent de 0, ce qui revient à dire que si le serial entré est différent du serial calculé, on affiche la boîte de message " Baaaaaaad password !! ". Si vous avez suivi les articles précédents, c'est du tout vu. Mais où sont stockés ces serials ? Nous devons trouver leurs emplacements mémoire pour pouvoir continuer.

IDENTIFICATION

On pose un breakpoint en 004014C5 (au début de la fonction " strncmp ") en appuyant sur F2, puis on appuie sur F9. Le programme se lance. On entre " toto " comme nom et " titi " comme serial. Le programme stope l'exécution au breakpoint. En appuyant deux fois sur F8, on arrive à la capture 2.

On remarque que s2, qui est la seconde chaîne de caractères passée en argument à la fonction " strncmp " est le password que l'on a entré. Mais quelle est cette chaîne s1 qui vaut " XEXE " ? Ce n'est pas notre serial. C'est donc le bon serial généré par le programme ! On a enfin trouvé le bon serial. Oui, mais ce n'est pas fini. On doit maintenant modifier le programme afin qu'il donne de lui-même le serial. On a vu tout à l'heure que le programme affichait une boîte de message. Nous allons nous en servir pour afficher le bon serial _. Voyons comment sont passés les arguments lors d'un appel d'une MessageBox (capture 3).

La première instruction PUSH 0 permet de définir le style de la boîte de message. Dans notre cas, elle contiendra seulement un bouton OK. Cela nous est indiqué par la présence de MB_OK

NGINEERING : ENNING

```
004014C5 | . 50              | PUSH EAX
004014C6 | . 8D85 F8FDFFFF  | LEA EAX,DWORD PTR SS:[EBP-208]
004014CC | . 50              | PUSH EAX
004014CD | . 68 20504000     | PUSH KEYGENPI.00405020
004014D2 | . E8 79180000     | CALL <JMP.&msvcrt.strncmp>
```

```
maxlen
s2 = "titi"
s1 = "XEXE"
strncmp
```

2

```
004014F3 | > 6A 00           | PUSH 0
004014F5 | . 68 DD134000     | PUSH KEYGENPI.004013DD
004014FA | . 68 F5134000     | PUSH KEYGENPI.004013F5
004014FF | . 6A 00           | PUSH 0
00401501 | . E8 1A190000     | CALL <JMP.&USER32.MessageBoxA>
```

```
Style = MB_OK|MB_APPLMODAL
Title = "very bad bad things..."
Text = "Baaaaaad password !!"
hOwner = NULL
MessageBoxA
```

3

du paramètre " Style ". Le paramètre " Title " est ensuite passé à la fonction, puis le texte " Baaaaaad password !! " stocké à l'adresse 4013F5. Pour afficher notre bon serial, nous allons juste changer le second argument de la fonction. Pour cela, nous allons remplacer l'adresse passée pour le paramètre " Text " par celle du bon serial (405020), et le tour sera joué, la boîte de message indiquera le bon serial à l'utilisateur. Nous allons aussi profiter de l'occasion pour changer le titre, stocké à l'adresse 4013DD, par " Voici le bon serial : ".

MODIFICATION

Première étape : connaître les adresses des codes hexas à modifier. Dans notre cas, on sait que l'on doit modifier le titre de la boîte de message stocké en 4013DD, ainsi que l'instruction PUSH 004013F5 en PUSH 00405020 qui passera comme paramètre " Text " à la fonction MessageBox notre serial à la place du texte " Baaaaaad password !! ". Cependant, nous ne savons pas quels codes hexas remplacer, ou écrire. Allez à l'adresse 004014FA, où se trouve normalement l'instruction PUSH 004013F5. Faites un double clic sur la ligne, et une boîte de saisie apparaît. Remplacez le PUSH 4013F5 par PUSH 405020 (capture 4).

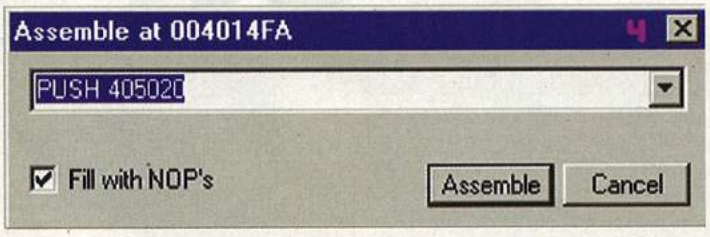
- **ADRESSE 004014FB : 20**
- **ADRESSE 004014FC : 50**
- **ADRESSE 004013DD : [NOTRE TITRE DE BOÎTE DE MESSAGE]**

Il ne nous reste plus qu'à trouver les offsets correspondant dans le programme, c'est à dire les adresses réelles où se trouvent ces codes hexadécimaux dans le fichier exécutable. Pour cela, on s'aide de WinDasm le bien nommé, qui nous donne ces informations :

- **OFFSET 8FB : 20**
- **OFFSET 8FC : 50**
- **OFFSET 7DD : [NOTRE TITRE DE BOÎTE DE MESSAGE]**

On n'a plus qu'à modifier l'exécutable, de telle manière qu'il nous donne le bon serial sans qu'on ait à coder quoique ce soit. Ressortons notre cher Ultra Edit (éditeur hexadécimal) de notre disque. On ouvre le fichier, et on va à l'offset 783h. On y écrit le nouveau titre de notre boîte de message, c'est à dire : " Voici le bon serial : ".

On modifie ensuite les codes hexadécimaux à l'offset 89C (capture 6).



Validez, et vous verrez ensuite ceci

```
004014FA |    68 20504000    | PUSH KEYGENPI.00405020
004014FF | . 6A 00           | PUSH 0
```

5

En rouge apparaissent les codes hexas modifiés. On note donc les modifications à effectuer, ainsi que les adresses (toutes les valeurs sont en hexadécimal) :

```
0007da | 20 21 00 56 6f 69 63 69 20 6c 65 20 62 6f 6e | !.Voici le bon
0007e9 | 20 73 65 72 69 61 6c 3a 00 2e 2e 00 42 61 61 | serial:....Baa
```

6

On enregistre, et on exécute ensuite le programme. On entre " toto " comme login, puis " titi " comme mot de passe. On observe le résultat dans la capture 7.

Notre modification marche très bien, et le programme donne tous les serials, pour n'importe quel login ! Les plus doués d'entre vous saurons sûrement coder un patch, un petit programme qui fera à notre place les modifications dans le programme exécutable (NB : un programmeur est fainéant, et laissera tout le boulot à ses programmes ...).

CONCLUSION

L'auto-keygenning est une méthode qui permet de simplifier le codage de keygens. Elle est considérée par les pros du cracking comme une technique d'amateurs, mais tant que le résultat est là, nous n'allons pas nous en plaindre. L'étape suivante serait de coder un keygen, mais vous n'avez pas encore toutes les notions pour arriver à cela. Pour le moment, avoir réussi cet autokeygen, c'est déjà pas mal ! À un prochain numéro de Pirat'z, au détour d'une page ...

Virtualabs

ALLEMAGNE : À LA TAXE !

Dorénavant, en Allemagne, il faudra payer une taxe (environ 12 euros) sur les PC achetés. Cette taxe respecte le même principe que celle réclamée sur les cassettes vidéo et les CD vierges : puisque le PC sert à pirater, il faut donc payer des droits d'auteur lors de l'achat. Il s'agit du premier pays à imposer cette taxe. Évidemment, les fabricants contestent cette loi. On ne sait pas encore si cette taxe sera appliquée seulement aux PC équipés d'un graveur, mais vu qu'on peut télécharger avec tous les PC, c'est mal barré...

HAK MA KDO NAD

Le site de McDonald's a été piraté le week-end de Noël parce qu'il traitait la Chine et Taiwan comme deux pays séparés. En effet, pour connaître les différents emplacements des restaurants, on y trouvait la Chine et Taiwan comme deux entités distinctes. La nuit de Noël, la page en chinois du célèbre restaurant n'était plus qu'un crâne noir et blanc qui disait : " protestez contre McDo qui prétend que Taiwan est indépendant ". McDo n'a pas intérêt à ce que les Chinois le boycottent puisqu'il s'agit d'un son huitième plus grand marché.

LAISSEZ TOMBEI ENREGISTREZ LE

Il y a beaucoup d'excellentes webradios sur le Net, mais écouter un flux continu de musique est parfois un peu contraignant. Ce serait quand même plus simple si les mp3 des morceaux tombaient directement sur votre disque dur, pas vrai ? Alors voici la solution.

KAZAA SUR LE DÉCLIN

Comme avec Napster, les autorités ont un train de retard, et continuent de taper sur leur adversaire Kazaa pourtant déjà bien mal en point. Ainsi, en Australie, un procès est en cours, visant à forcer Kazaa à bloquer les téléchargements illégaux. De son côté, Kazaa dit : " on a déjà essayé mais ça ne marche pas ", mais prétend aussi par ailleurs : " on est capable de bloquer les pédophiles ". L'avocat adverse en déduit qu'ils peuvent aussi bloquer les téléchargements illégaux. À moins que leur blocage des pédophiles ne fonctionne pas.

BITTORRENT TOUJOURS AU TOP

C'est confirmé, BitTorrent est bel et bien LE logiciel préféré des internautes pour télécharger des films (ou des séries TV) sur le Net. Certes, eDonkey est toujours là, mais en termes de bande passante, il n'y a pas photo : un analyste anglais estime que BitTorrent représente plus du tiers du trafic internet total (voyons... un tiers pour BitTorrent, un tiers pour les spams, un tiers pour les films de cul, ça ne laisse pas grand-chose pour télécharger ses MP3 !). Dans un article de Wired.com, on en apprend un peu plus sur le créateur, Bram Cohen. Déjà, qu'il gagne bien sa vie grâce à BitTorrent (je hackerais bien son compte Paypal), ce qui pourrait vous donner des idées. Mais avant de vous essayer à trouver un protocole de partage encore plus performant, sachez que Bram est un peu autiste sur les bords, et fana de casse-tête que vous ne seriez pas capable de résoudre en 6 mois quand il n'a besoin que de deux jours. Remarquez, quand je vois vos emails, je pense qu'il y a quelques autistes parmi nos lecteurs, ça serait donc fort possible !

Les webradios diffusent leurs programmes en streaming, qui est un flot d'informations continu. Il existe plusieurs technologies : shoutcast, icecast, peercast ou les formats real et windows. Vous trouviez d'ailleurs, dans le dernier numéro spécial de Pirat'z, les explications détaillées pour faire une webradio " shoutcast ".
Un annuaire vraiment conséquent de webradios utilisant cette technologie est disponible sur http://www.shoutcast.com/. On se rend compte que de nombreux genres musicaux sont diffusés en différentes qualités. Seulement, écouter la radio c'est sympa, mais il faut être connecté sur le Net...
Depuis décembre, un nouveau plugin winamp (c'est un programme qui ajoute une fonctionnalité à un programme déjà existant), permet d'enregistrer les webradios aux formats mp3 et ogg, de découper les morceaux, et de les renommer automatiquement. Comme les cassettes audios à l'époque, ce logiciel permet donc d'écouter ou de réécouter les morceaux en différé.

C'EST LÉGAL !
En vertu du droit à la copie privée, vous avez tout à fait le droit d'enregistrer un morceau qui passe à la radio, pour votre usage personnel; et c'est vrai aussi sur le Net. Mais si vous avez le droit de posséder des mp3 ainsi rippés, il est par contre illégal de les diffuser sans autorisation, par p2p ou autre.

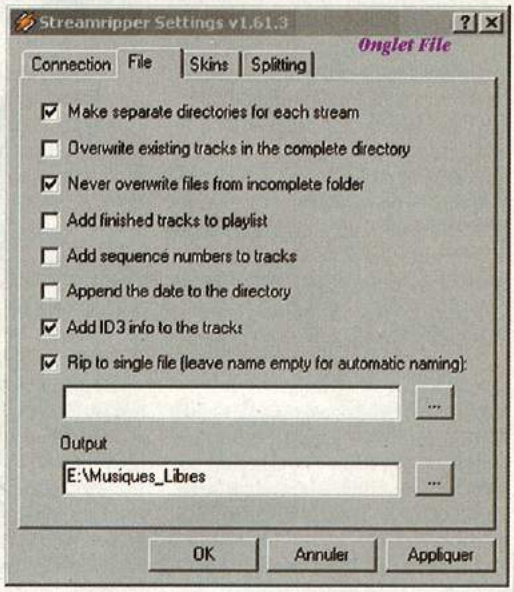
INSTALLATION

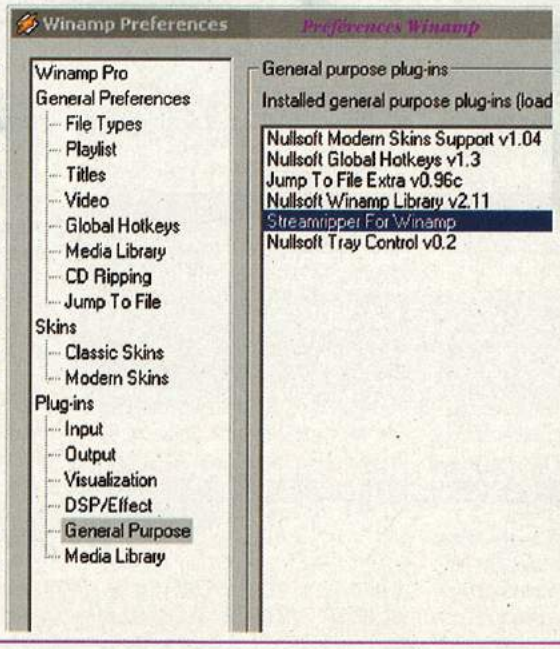
Tout d'abord, il faut winamp (http://www.winamp.com/), ensuite il faut télécharger Streamripper sur sourceforge (http://streamripper.sourceforge.net/, rubrique download, puis streamripper winamp 2/5 plug-ins; chouette, c'est du libre !). Lors de l'installation, Streamripper va rechercher winamp, et s'ajoutera dans ses fonctionnalités.
Vous le trouverez dans les préférences de winamp (ctrl+p) : cherchez plug-in puis General Purpose. Une ligne devrait s'intituler Streamripper for Winamp ; sélectionnez-la, puis cliquez sur configure selected plug-in. Une fenêtre winamp s'ouvre. Il est aussi accessible dans la barre des tâches, à gauche de l'heure.

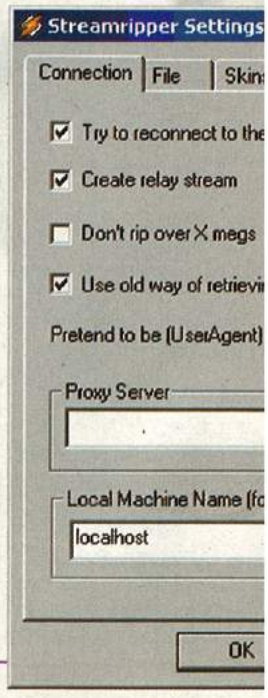
CONFIGURATION

Dans L'onglet file il y a plusieurs options en english. Voici les plus intéressantes.

Make separate directory for each stream :
Cette option crée un répertoire différent pour chaque webradio enregistrée. Ceci permet de savoir d'où viennent les mp3 enregistrés.
Add IDv3 infos to the tracks :
Rajoute les informations supplémentaires envoyées par la webradio parmi les infos incluses dans les fichiers mp3.
Rip to single file :
Permet d'enregistrer le flux dans un fichier unique, plutôt qu'en fichiers séparés.







R LE P2P, ES WEBRADIOS !

Output : Permet de définir le répertoire dans lequel les fichiers seront enregistrés.

Try to reconnect to the stream if it drops :
Essaye de se reconnecter à la webradio s'il y a eu un problème de réception.

Create relay stream :
Crée un relai local, ce qui permet d'éviter que de vous connecter deux fois à la webradio (une fois pour écouter la radio dans winamp, et une autre fois pour l'enregistrer avec le streamripper ou depuis un autre poste du réseau local).

Don't rip over X mepgs Megs :
Permet de limiter la taille totale des fichiers enregistrés. Utile si vous vous éloignez de votre ordinateur pendant plusieurs heures - ou jours ! Précisez l'espace maximum en mégaoctets.

Use old way of retrieving the current **track from winamp :**
À cocher si l'attribution du nom des fichiers ne fonctionne pas.

Pretend to be (UserAgent) :
Permet de tromper les webradios qui refuseraient la connexion de streamripper ; mettre " winamp 3.02 " ou " windows media player ".

Proxy Server :
Pour les paranos qui voudraient utiliser un serveur intermédiaire entre la webradio et eux, ou ceux qui y sont forcés (intranet, etc.).

Local Machine Name :
À préciser si l'option Create relay stream est cochée (localhost, 127.0.0.1 ou l'ip locale de la machine).

L'onglet splittingpermet de modifier le mode de découpage des fichiers. Les webradios diffusant des morceaux mixés, il est possible que sur un mp3 on entende la fin du morceau précédent et le début du suivant. Le fonctionnement en mode standard est vraiment satisfaisant si l'on utilise un mode de mix automatique lors de l'écoute des morceaux (crossfader automatique Ctrl+P, plug-in Output).

Vous pouvez malgré tout modifier les options si vous pensez pouvoir faire mieux que la configuration par défaut. L'onglet skin (peau) permet de définir l'apparence du plug-in. c'est juste pour faire joli.

ENREGISTREMENT

Très très simple : lorsque vous écoutez une webradio, la fenêtre du plug-in affiche " press start to rip ". Il suffit d'appuyer sur start et le programme musical sera enregistré et découpé selon votre configuration dans le répertoire que vous aurez précisé.

Streamripper fonctionne avec les radios aux format mp3, ogg (encore incomplet), shoutcast/icecast, nvs (nullsoft), aac. On peut aussi enregistrer un flux peercast en branchant Streamripper sur le relai local de la station.

Plus d'informations :
http://streamripper.sourceforge.net/
http://winamp.com/
http://www.winampfr.com/

Annuaires de webradios :
http://www.shoutcast.com/
http://www.comfm.com/

Aliskovitch

IZ

PIRATES CHEZ MICROSOFT

C'est le genre de nouvelles qu'on aime toujours, quand on peut taper un peu sur le dos de notre ami Billou. Si vous avez XP, ouvrez le bloc-notes, puis éditez n'importe quel fichier .wav dans Windows \ Help \ Tours \ WindowsMediaPlayer \ Audio \ Wav, et regardez tout à la fin. Vous voyez le nom " DeepzOne " ? Il s'agit du nom d'utilisateur enregistré dans Sound Forge 4.5, qui a servi à créer ce fichier. Qui est DeepzOne ? Un fondateur du groupe de crack de logiciels audio Radium. MS utilise donc un logiciel piraté, ou emploie un pirate ?

OVERPEER VOUS SOUHAITE UNE BONNE ANNÉE

Si vous avez oublié qui sont nos bons amis d'Overpeer, je vous le rappelle en deux mots : des emmerdeurs. En plus de mots : des gens très bien intentionnés qui veulent combattre le méchant P2P en causant un maximum de problèmes à ses utilisateurs. Leur dernière trouvaille : exploiter une faille (pas encore corrigée) dans la gestion des licences DRM (Digital Right Management) par Windows Media Player. Cette faille permet d'utiliser DRM pour accéder à une page web quelconque (par exemple contenant un exploit relatif à Internet Explorer, une idée qui plaît beaucoup aux hackers) à la lecture d'un fichier. Normalement, c'est censé servir par exemple à n'autoriser un fichier à être lu qu'un certain nombre de fois. Ici, Overpeer l'utilise pour charger une page qui bombarde le pauvre internaute de messages publicitaires, essaie d'installer des spywares, de rajouter des favoris et de changer la page d'accueil d'IE. Voilà qui va nous faire encore plus aimer Overpeer, Microsoft, et surtout le format audio WMA (vous n'aurez pas ce problème avec des MP3).

HACKEZ VOTRE CALCU

2004, UNE BONNE ANNÉE

Pour les virus en tout cas ! C'est ce qui ressort d'une étude qui montre que le nombre de virus dans la nature a augmenté de 50 % en 2004 par rapport à 2003. Parmi les caractéristiques prédominantes de l'année virale 2004, notons les " bot-nets " (réseaux d'ordinateurs zombies infectés servant au spam ou aux attaques de déni de service), le premier " vrai " virus pour téléphones portables, le virus Netsky, vainqueur du " Masters " des virus, et le SP2 de Windows XP, qui a réussi à planter plus d'ordinateurs que tous les virus réunis.

MUSIQUE, P2P, GRATUITE, LÉGALE

Généralement, on a du mal à mettre tous ces mots ensemble dans un même logiciel. C'est pourtant ce que nous promet Mercora (www.mercora.com), un logiciel de radio P2P au principe assez prometteur. L'idée est de permettre à chaque ordinateur du réseau P2P de diffuser de la musique. C'est donc différent du partage de fichiers, puisqu'il est impossible pour les auditeurs de télécharger les morceaux sur leur disque dur (enfin, en théorie, des logiciels pour faire ça vont sûrement apparaître). Grâce à cela, à des accords passés avec les labels et des publicités passées sur votre ordinateur, Mercora peut rester gratuit tout en étant légal, ce qu'on n'avait pas vu depuis un fameux poisson d'avril l'an dernier. Mais tout n'est pas rose bonbon dans le monde de Mercora : déjà, il est impossible de chercher une chanson particulière, ou de demander à ce qu'elle soit jouée, car le service doit être non-interactif pour être légal. De plus, un service " premium " payant doit apparaître bientôt. Difficile donc de savoir ce que " gratuit " signifiera dans le futur...

Le hacking est une affaire de curieux, vous commencez à le savoir. C'est pourquoi nous avons décidé de ne pas nous arrêter aux ordinateurs de bureau : il est possible de faire des expériences très intéressantes avec une simple calculette !

Tous les connaissez probablement : les calculatrices graphiques Casio. Elles existent depuis longtemps et nombreux sont les développeurs qui ont tapé leurs premières lignes sur ces machines. Répandues et simples d'utilisation, elles permettent d'assimiler facilement les concepts de variables, boucles et conditions. Au fil du temps, les bugs et astuces se sont accumulés. Nous allons tenter d'en faire une synthèse. Nous ne traiterons ici que des Graphs 30 à 100 / 100+ en nous concentrant notamment sur ces deux dernières.

I] THÉORIE

Structure de la mémoire d'une Graph 100

La Graph 100 peut être assimilée à un ordinateur car elle en possède :
- le processeur (un Nec V30Mx qui tourne à 8 Mhz),
- la mémoire vive (la RAM, elle en possède 256 ko),
- la mémoire de stockage (qui est ici une mémoire dite flash et non un disque dur),
- le bios (un T-Note Bios v0.60 r1.10),
- le système d'exploitation : Rom-Dos 6.2 [1] compatible à 100 % avec Ms-Dos.

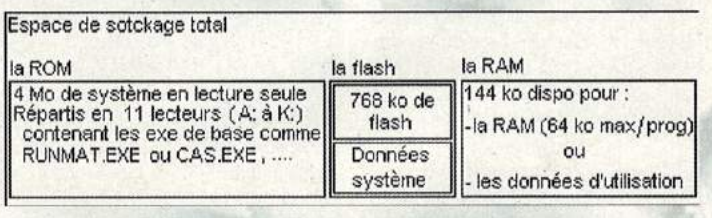
La mémoire de stockage est divisée en deux parties :

- la ROM (4 Mo) où sont stockés les langues, les menus constructeurs et surtout le système : des lecteurs de tailles variables allant de A:\ (lecteur de boot) à K:\- la mémoire flash qui comprend :
- une zone de " stockage " : 768 ko répartis en six lecteurs de 128 ko allant de L:\ à Q:\,
- mais aussi une zone système, une copie du lecteur A:\, la langue utilisée et une zone vide.

Cette zone système peut être lue et modifiée (pour permettre le rajout d'icônes ou la modification du design). Vous vous demanderez peut-être : " Mais où se trouvent mes programmes basics (mes pompes de maths par exemple) ? " La réponse est simple, ils se trouvent dans la RAM qui peut être utilisée comme :
- zone de stockage (jusqu'à 144 ko) où sont situés les programmes basics, variables, graphs ou encore les matrices,
- RAM en tant que telle (mémoire vive servant à l'exécution de programmes...).

À savoir qu'aux vues de l'étroitesse de la RAM, Rom-Dos limite la mémoire à 64 ko par programme !

Le stockage des programmes basics dans une mémoire volatile explique pourquoi toutes les données de type programmes, graphes, listes... sont effacées lorsque les piles (et piles de sauvegarde) sont retirées.
Pour plus d'information, consulter " Le guide du programmeur " pour la Casio Graph 100 [2].
Pour simplifier, voici un schéma :



Toute cette théorie sera notamment utile pour les développeurs de flashes : vous savez, ces icônes supplémentaires qui se rajoutent dans les Graphs 100 / 100+.

Approche du langage utilisé

Les Graphs utilisent une version (très) simplifiée du basic.

Voici un exemple de programme.

```
' notez que les commentaires
' commencent par une apostrophe
' on entame une boucle de 1 à 7
' (variable : I)
For → I  To 7
' on affiche un texte à partir du début
' (colonne 1), ligne I
Locate,I,"Je suis le "
' on affiche un texte à partir du
' caractère 14, ligne I
Locate,I,I
' on ferme la boucle
Next
' on exécute...
Do
'... rien ...
' tant que la touche 78 (Shift) n'est
' pas pressée
LpWhile Getkey ≠ 78
```

Ce qui équivaut en C à :

```
int main () {
 int i;
 for (i=0;i<=7;i++)
  printf("Je suis le %d\n",i);
  getchar();
  return 0;
}
```

Voici un petit mémo des instructions les plus utilisées.

Les variables :

L'affectation des variables se fait via cette syntaxe : valeur _ variable.
Attention, il n'y en a que 26 et elles ne peuvent contenir que des valeurs numériques.
Il est aussi possible d'utiliser r et Xmax, Xmin, Xscale, Y1... pour disposer de quelques variables supplémentaires :-)
Les opérateurs Isz et Dsz permettent d'incrémenter ou de décrémenter une variable.

Les entrées-sorties texte :

Avec 7 lignes de 21 colonnes en mode texte, l'écran ne permet pas des merveilles. Pour obtenir une valeur d'un utilisateur, utilisez le " ? ".
Pour afficher le contenu d'une variable : var ▲(par exemple A▲).
Pour écrire, on peut taper : " BONJOUR " ou encore Locate x,y, " BONJOUR " pour spécifier un emplacement.

ETTE CASIO !

Les conditions :
Jusqu'aux Graphs 80, ce symbole " => " permettait de faire une condition simple (une seule conséquence) notamment utilisé pour faire un saut conditionnel de ce type :
A=3 => Goto 1

Désormais disparu, il faut utiliser ce modèle un peu plus lourd :
```
If condition
Then conséquence1
conséquence2 ....
IfEnd
```

Les boucles :
Toujours les grands classiques, seule la syntaxe diffère légèrement.
- `For val1 → variable To val2 (Step 3) .... Next`
- `Do... LpWhile condition`
- `While condition ... Whilend`
- `Lbl numéro ... Goto numéro`

Et voici un autre bout de code pour exprimer plus concrètement ces principes :

```
?_A
If A=12345
Then A-2345_A
IfEnd
A▲
```

Les touches :
Comme sur un ordinateur, chacune d'entre elles possède un code qui lui est propre, pour les Casio :
- pour une touche à droite, le nombre est décrémenté de 10,
- pour une touche en bas, le nombre est décrémenté de 1,
- le code de la touche F1 est 79,
- les flèches du haut, du bas, de gauche et de droite valent respectivement 28, 37, 38 et 27.

Ceux qui ont compris savent désormais que la touche EXE a pour code 31.
Pour récupérer tous les codes de touches :
```
Do
GetKey→K
Locate 1,1,K
Locate 1,1,"  "
LpWhile 1
```

À savoir : la touche AC/on est indépendante (dommage :-).

L'écran :
En mode graphique, on dispose de 127x63 (soit 8001) pixels utilisables.
Les coordonnées des points dépendent du ViewWindow.
`ViewWindow 1,127,0,1,63,0` définit que le point (1,1) se trouve en bas à gauche.
À noter que les Graphs 100 / 100+ ne permettent plus d'avoir une fenêtre aux coordonnées inversées (1 à droite et 127 à gauche).
Pour y écrire :
`Text 1,20,"BONJOUR".`
Les plus assidus auront vu la syntaxe est sous cette forme Text y, x et ne dépend jamais du ViewWindow.
Sachez qu'il est bon de laisser 6 à 8 pixels d'écart entre deux lignes horizontales lors de l'utilisation de Text.

II] PRATIQUE

Les menus cachés

Après tous ces aspects techniques et cette théorie (qui vous servira tout de même pour programmer :-), passons à la pratique.
Tout comme les palms ou téléphones portables, les calculatrice Casio ont leurs " menus constructeurs ".

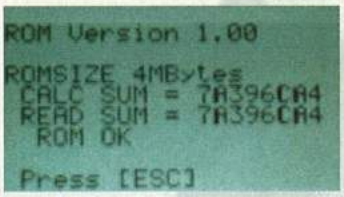
Le plus connu s'obtient par l'appui simultané des touches
F6 - a+b/c - AC/on
Le voici sur une graph 60/65 :

Et sur graph 100 / 100+ :

Attention ! On commence les choses sérieuses, à votre place, je sauvegarderais toutes mes données car un accident est très vite arrivé.

Pour quitter ce menu sans encombre, appuyez sur 0 (" Reset ") puis choisissez " No ".

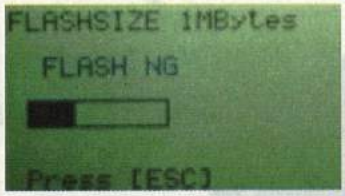
Dans ce menu, on peut, en vrac, tester le contraste (CONT), les pixels (LCD), les touches (KEY), les piles (DET) et la transmission (TRANS)...



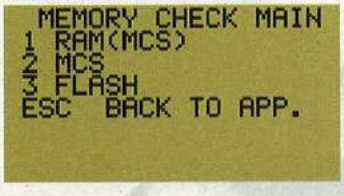
... ou encore la version de votre ROM (1.00 pour les Graphs 100, 1.02 ou 1.03 pour les 100+).
Attention : tester la RAM efface vos basics et tester la Flash efface vos flashes.

D'ailleurs, si vous connaissez quelqu'un qui ne peut pas se débarrasser de ce message au démarrage :

Alors, testez sa flash. Et si ce message s'affiche (comme ici sur la Graph de mon petit frère) :



... c'en est fini de votre calculatrice :'((la mémoire flash est morte).
Un second menu spécifique aux Graphs 100 / 100+ et dont l'existence a été révélée plus récemment ressemble à ceci :
Comme nous allons le voir, il est d'une grande utilité pour... les mots de passe.



'Z

Le spam en baisse

C'est AOL qui le dit. Grâce à leurs efforts pour combattre les spammers, ils sont passés de 2,1 à 1,6 milliard de spams par rapport à l'an dernier. Ils ont aussi reçu 75 % de moins de plaintes de la part de leurs abonnés. Ce qu'on peut déduire de ces chiffres : AOL a de moins en moins d'abonnés, et intéresse donc de moins en moins les spammers, d'autre part, leurs abonnés ont enfin compris qu'envoyer des plaintes ne servait à rien, puisque le fils du dictateur du Boungour réapparaissait aussitôt en neveu du président du Yéméné.

Une faille, deux failles, trois failles... Piraté !

Microsoft peut bien se plaindre du manque de discernement de certains chercheurs en sécurité, c'est quand même leur faute si Windows a plus de failles que l'océan Pacifique. Ainsi, le groupe de sécurité chinois Xfocus a dévoilé sur son site web trois nouvelles vulnérabilités dans Windows, pas encore patchées par Microsoft au moment d'écrire cette news. La plus intéressante concerne l'API LoadImage de Windows, qui est utilisée notamment dans IE ou Outlook, et peut être exploitée par une page web ou un email affichant une image corrompue. Il s'agit d'un type de vulnérabilité de plus en plus populaire : l'integer buffer overflow, c'est-à-dire un buffer overflow causé par un entier prenant une valeur inhabituelle (par exemple, si un entier sur 16 bits prend ses valeurs entre -32768 et 32767, rajouter 1 à 32767 va donner -32768, ce qui peut perturber sérieusement un programme selon ce qu'il fait ensuite du résultat). Les deux autres vulnérabilités concernent respectivement la gestion des curseurs animés (fichiers .ani) et des fichiers d'aide. Bonne année !

Récupération de mot de passe Pour les Graphs 30 à 80

Le principe consiste à créer une erreur dans la RAM en la chargeant au maximum afin d'en visualiser le contenu.
Voici concrètement comment procéder :

- notez tout d'abord le nom du programme protégé,
- créez une matrice de grande taille (genre 50x38) pour qu'il ne reste qu'un peu moins de 5500 octets de mémoire (cette dernière est visible dans la rubrique " MEM " : lettre E),
- dans le menu 6 (Dyna), créez un graph (pas trop compliqué, du style Y=AX) mais sans le lancer ! En effet, c'est un programme qui va s'en charger,
- un atout des programmes est que lorsqu'on les " breake " en l'absence de mot de passe, le programme est édité pour faciliter le débogage, or, dans notre cas et à cause de la surcharge de la mémoire, le programme ne sera pas édité. Donc, pour ce faire, créez un programme et insérez-y uniquement DrawDyna (Programme (Shift+Vars) > F6 > Disp (F2) > Dyna (F3)),
- attendez le chargement et une fois le graph en mouvement, stoppez-le (à l'aide de la touche AC/on) puis appuyez sur une flèche de direction,
- surprise : ce n'est pas votre programme qui se trouve édité mais quelque chose de bien plus étrange peuplé de symboles ésotériques :o! (sommes-nous dans la matrice ?),
- Attention, à partir de maintenant, ne touchez qu'au curseur (ou à Exit) ! Dans le cas contraire, vous auriez droit à un magnifique Sys Error qui, au mieux, vous bloquera dans votre quête et, au pire, endommagera votre RAM, vous obligeant à un petit Reset. D'autre part, si vous laissez la calculatrice s'éteindre, vous reviendrez dans le menu principal au prochain allumage :-\

Cette partie est la plus laborieuse car il vous faut parcourir plusieurs kilo-octets de terrain inconnu. Pour cela, faites remonter le curseur au maximum. Il arrive que celui-ci se bloque quelques secondes avant de réapparaître plus bas,

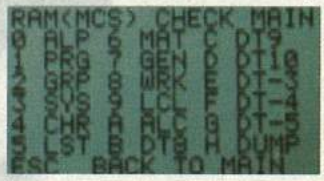
- après une demi-heure de cours de maths passée le nez sur votre écran, vous devriez voir apparaître quelque chose ressemblant à ça :

Attention, le mot de passe est représenté à l'envers (BANANE deviendra ENANAB), gare à ne pas le rater en cas d'inattention (surtout, ne vous laissez pas perturber par le cours de maths !) car tous vos efforts auraient alors été vains...

Pour les Graphs 100 / 100+

Pour le coup, les ingénieurs de chez Casio ont été d'une extrême gentillesse et nous ont permis de récupérer les passes en moins d'une minute grâce aux menus secrets qui trouvent alors une certaine utilité.

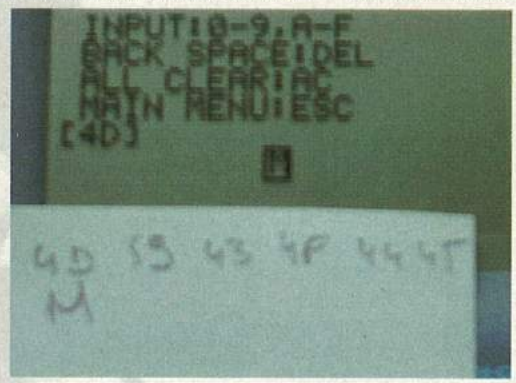
- commencez par noter la position (selon l'ordre alphabétique) du programme rebelle,
- puis rendez-vous dans le menu constructeur s'obtenant via F6 - a+b/c - AC/on,
- appuyez deux fois sur 1 (RAM > PRG) et descendez le nombre de fois nécessaire pour tomber sur le programme codé (sa 4e ligne est différente d'une suite de 0),



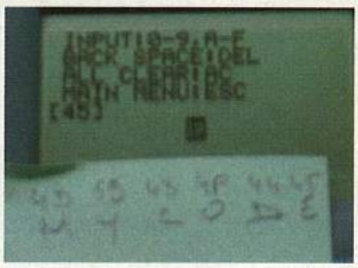
-en effet, notez bien cette 4e ligne car c'est le mot de passe, mais les lettres sont converties en leur équivalent numérique :-(

- pas de panique, les ingénieurs de Casio nous ont offert le convertisseur en série !
- une fois le pass " crypté " en poche, il suffit de se rendre dans le menu constructeur " classique " (F6 - a+b/c - Ac/on) et d'appuyer sur F1 (magique),
- on y entre le code des caractères et ceux-ci apparaissent !

Le premier puis, de fil en aiguille...



le mot de passe en entier



Apparemment, l'affichage pose quelques problèmes et certains symboles sont mal représentés, ce qui est le cas avec les symboles suivant :

-, /, x, r

Cela pourrait décourager le premier venu, mais sera vite déjoué par quelqu'un d'averti.
Moralité, sur Casio, mieux vaut coder " open-source "... de toute façon, vous n'avez pas le choix :-)

Les bugs

Pour finir, voici quelques bugs (largement répandus) qui affectent les Graphs 30 à 80.
La calculatrice part dans une boucle infinie ce qui force l'appuie sur Reset pour la redémarrer.

```
Lbl 0
For 1→A To 0
Goto 0  Lbl 0
Do
Break
Goto 0  Lbl 0
While 0
Goto 0  For 1→A To 0
Lbl 0
Goto 0  While 0
Lbl 0
Goto 0  Do
Lbl 0
Break
Goto 0
```

Aucun d'entre eux ne fonctionne sur une Graph 100 qui analyse syntaxe et boucles avant l'exécution proprement dite. Mais je vous présente une technique en exclusivité qui va changer la face du monde !
J'ai écrit ce code de manière totalement hasardeuse et malgré quelques améliorations par la suite, je pense qu'il est tout de même réductible. D'ailleurs je m'interroge toujours sur l'origine réelle du plantage :|

```
Lbl
Text,50,"OWNED !"
Cls
Do
While
Do
Do
While
Break
WhileEnd
Do
Do
Break
Do
Do
Do
WhileEnd
LpWhile
LpWhile
LpWhile
LpWhile
LpWhile
LpWhile
LpWhile
LpWhile
LpWhile
Goto1
```

Nous n'avons volontairement pas parlé concrètement des " flashes ", mais vous disposez désormais des bases pour les comprendre. Sachez qu'elles se développent en Asm/C++ à l'aide de quelques librairies. Si cela vous intéresse, allez faire un tour sur les sites ci-dessous. Avec un peu de patience et de motivation, vous serez peut-être l'auteur du prochain jeu grand public sur Casio (et votre tête sera mise à prix par tous les profs de maths :-). Toutefois, gardez à l'esprit qu'une calculatrice reste un outil et non une Game Boy ;-)

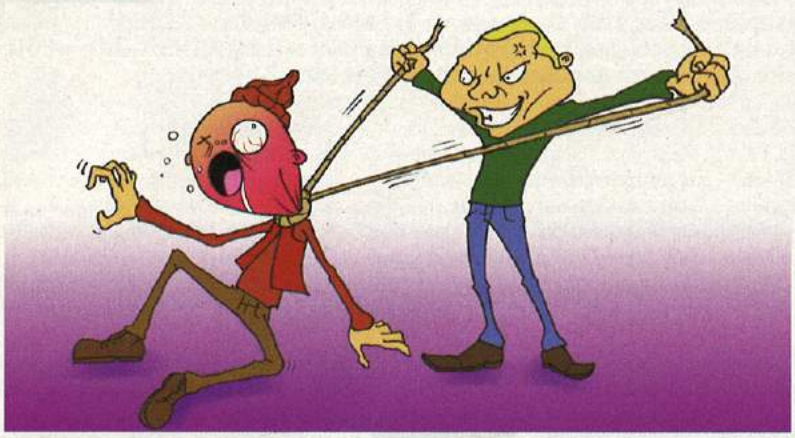
III] LIENS

[1] Rom-Dos : http://www.data-light.com
[2] Données techniques et théoriques indispensables : http://www.gprog.tk
L'incontournable : http://www.graph100.com/
Pour la kiwi compil (compilation de plusieurs flashes d'installation facile) : http://kiwicasio.earthforge.com
Des tutoriaux sur les transferts et de très bonnes flashes : http://www.na-prod.com/index.php?page=casio
L'auteur de " Touche " : http://www.2072productions.com
L'excellente team de développeurs : http://fgpstudios.free.fr
http://www.casioworld.fr.st/ (de nombreuses infos en tout genre)
http://www.casioland.net/trucs_astuces.php (de nombreux basics bien classés)

Gros-Bibi

A MORT LES SYSTEMES D'INFORMATIONS !

La LCEN a fait bouger pas mal de monde, à commencer par l'association francaise des fournisseurs d'accès qui ont fait pression, et par la ligue Odebi qui lançait une pétition en ligne. Pourquoi tant de révolte ? C'est enfantin : la LCEN propose de restreindre nos droits sur l'Internet.



L'adoption par le Sénat de la LCEN (Loi pour la confiance en l'économie numérique), après ratification, a mis le feu au poudres. On pouvait bien sûr être certain que l'opposition serait faible, vu la publicité faite pour cette loi. Contraste flagrant avec celles concernant la modification des congés, ou autres changements. Cependant, cette loi se révèle être " fourre-tout ", d'après ce qu'en disent des informaticiens membres de la ligue Odebi - www.odebi.org. Elle aurait même été commandée par les lobbies des majors. J'ai voulu m'en assurer par moi-même. Plongée dans le monde réel.

PREMIERS CONTACTS

Sachant pertinemment qu'ils possèdent une section spécifique aux crimes relatifs à l'Internet, je me suis tout d'abord attaché à prendre des renseignements auprès de la gendarmerie nationale. J'ai donc composé le numéro de la brigade de ma ville, et suis tombé sur le standardiste. Je lui ai exposé mon cas, en lui disant que je suis webmaster d'un site, et que je tenais à avoir quelques renseignements sur ce que je pouvais mettre comme contenu, mon site traitant de sécurité informatique. Le pauvre homme m'a rabâché la loi Godfrain. Aucune trace de la LCEN. Je l'ai remercié poliment, et lui ai demandé toutefois, avant de raccrocher, qui d'autre je pourrais joindre. On m'a dit d'appeler à la police nationale, ils devraient pouvoir me répondre.

Beaucoup d'appels en vain. Après quelques heures passées au téléphone, il s'avérait finalement impossible d'obtenir des renseignements la concernant. Comment vouloir faire appliquer une loi si personne ne peut renseigner les personnes concernées ? Qu'est-ce que peut faire un webmaster pour être sûr de rester dans la légalité, avec comme seule base un texte de loi aussi obscur ?

Un samedi, j'ai rencontré un ami qui écrit dans un journal local et dont les parents bossent dans la police nationale, sa mère est conseillère juridique. Elle s'occupe notamment des applications de loi, et a aussi entendu parler de la LCEN. J'allais enfin pouvoir obtenir des renseignements fiables.

UN AUTRE POINT DE VUE

Après entretien, la mère de mon ami a fait ressortir deux points principaux, qui justifient cette loi. Le premier point sur lequel elle a insisté sont les articles de la LCEN concernant la pédophilie. Je concède tout à fait que filtrer le contenu des sites pour éviter ce genre d'abus, tout ce qu'il y a de plus abjecte, est réellement justifié. Elle mentionne aussi le fait qu'un pédophile a été arrêté et mis en examen dans ma ville, et ce, grâce à des traces laissées sur Internet. Pour démanteler ces réseaux, il faut disposer des moyens juridiques nécessaires, et la LCEN offre une liberté d'action plus grande aux enquêteurs. Et donc de meilleurs moyens pour lutter contre la pédophilie. Le second point évoqué est le piratage de droit d'auteurs. El le m'a rappelé que l'industrie du disque est en crise, que les ventes chutent et que bon nombre de personnes ne se rendent pas compte des conséquences d'une copie de CD pour un ami.Je l'ai laissée continuer, et c'est quand elle a abordé la sécurité informatique que c'est devenu intéressant.

PARADOXE OU PARANOÏA ?

Elle m'a donc affirmé que si l'on enlève les espaces de publications de failles, on réduira considérablement le nombre de piratages sur Internet, du moins ceux en rapport avec le territoire français. Je lui ai expliqué mon point de vue : si l'on supprime ces sites de publication de failles, on ne peut faire qu'augmenter le nombre de piratages, car les correctifs de sécurité ou les mises à jour ne seront plus faits à temps, faute d'information. Sans participants maîtrisant les techniques d'attaques, la communauté du libre ne peut pas trouver de failles, et donc stagnera. Ce serait la fin des haricots. Contrairement à ce que je pensais, elle a approuvé ce que j'ai dit mais que sur un seul point : celui des updates et patches. La communauté, quant à elle, passe en second plan. J'en suis arrivé tranquillement au point que je voulais aborder, celui du paradoxe sécuritaire. Je lui demandais donc si à force de vouloir sécuriser au maximum on n'encourageait pas à l'attaque. Car si les personnes qui cherchent les failles ne peuvent plus les dévoiler, on crée une rupture entre eux et les éditeurs de logiciels par exemple, en favorisant aussi une circulant unilatérale des exploits. Ce qui implique un accroissement des attaq ues. Elle a été embêtée. Je l'ai conduite dans une impasse. Elle m'a répondu gentiment que non, elle ne pensait pas que cette loi favorise le piratage, car son but est, entre autres, de combattre ce même piratage. Je l'ai remerciée poliment, et lui ai souhaité une bonne soirée.

Pour résumer notre conversation, il semblerait que la partie de la loi concernant la sécurité des systèmes d'information ait été ajoutée pour mettre à jour la loi Godfrain. Et principalement à propos des problèmes concernant le p2p ainsi que les violations de droits d'auteurs. Je n'ai pas eu d'informations concernant les conditions d'ajout des articles relatifs à la possession d'outils permettant le désassemblage par exemple, ou encore à ceux relatant la pub lication de failles. C'est dommage. Mais un pauvre rédacteur écrivant dans Pirat'z ne mérite pas de recevoir de telles informations. Pour éviter la paranoïa, je crois que je vais me recycler, laisser l'informatique de côté. Si c'est voué à un échec législatif, si une communauté existant principalement sur le web n'a plus le droit de publier les erreurs trouvées, de tester ce qu'avancent les éditeurs de logiciels, je pose cette simple question : où va-t-on ? Qu'a-t-on à gagner d'un monde où les éditeurs de musique, de logiciels ne peuvent plus être mis en cause ? On cherche des réponses auprès des utilisateurs, sans pour autant aller voir du côté des éditeurs. C'est aberrant de voir comment nous, simples utilisateur s et consommateurs, sommes les cibles d'une paranoïa sans précédent. Pourquoi acheter quand le libre nous donne ce qu'il a de mieux, ce qu'il a mis du temps à engendrer : des outils aussi performant que les grands " propriétaires ", et cela sans y mettre de prix. À toute cette communauté, je dis merci. Aux autres, je ne dis rien, et promet juste que l'on en reparlera dans quelques années, histoire de voir si cette loi a porté ses fruits. On dirait tout de même qu'ils donnent au Web la même image qui prend chaque jour une place plus grande dans nos vies : un espace commercial où tout est soit consommateur, soit consommation. Quittez vos ordinateurs, abandonnez vos claviers, l'équation internet=liberté n'est plus vraie.

Virtualabs

LES REPRIS DU HACKING

Que vous vous disiez blackhat ou whitehat, vous serez peut-être un jour confronté à ce qu'ont vécu les interviewés de ce numéro. En effet, Pirat'z a rencontré pour vous trois hackers ayant eu des problèmes avec les autorités, allant du simple administrateur système à de haut gradés du gouvernement français...

Les trois personnes interviewées ont voulu rester anonymes. Pour ceux qui côtoient la scène francophone, vous les connaissez peut-être sous un autre pseudo, peut-être même personnellement, qui sait ? Ils ne sont pas plus fous que d'autres, pas plus inconscients, ils ont pris des risques et se sont fait prendre.
Vous allez voir dans cet interview que quelles que soient vos intentions, vous n'êtes pas à l'abris de poursuites, pour peu qu'un administrateur système soit de mauvais poil. Vexé ou blessé, l'administrateur système qui reçoit un mail annonçant une faille de sécurité sur son système ne le prend pas toujours bien...

ANONYME1 : INTRUSION DANS LE SYSTÈME D'ADMINISTRATION DE SON LYCÉE. PEINE : UN BLÂME, UNE INTERDICTION D'APPROCHER UN PC APPARTENANT À SON LYCÉE PENDANT 6 MOIS.

PIRAT'Z : Ttu es le premier interviewé et ta peine est la moins grave des trois. Raconte-nous un peu ce qui s'est passé.

ANONYME1 : Avec quelques amis du lycée, on s'ennuyait entre midi et deux heures. Nous avons commencé à installer des jeux dans notre salle informatique et on se faisait des petits concours. Bien que ce soit interdit, ce n'était pas bien méchant. Un jour, l'administrateur à bloqué les exécutables sur les PC du lycée. Très perturbé par cette décision, nous avons cherché un moyen de jouer quand même (logique !). Cet administrateur avait mal réglé les accès sur certains ordinateurs et, après quelques manipulations, nous avons eu accès à son propre PC, qui bien sûr ne bloquait pas les exécutables. Nous avons donc installé le jeu sur son ordinateur et nous jouions à distance. C'est complètement débile quand on y repense. On en a profité aussi pour choper tous les mots de passe des professeurs...

PIRAT'Z : Il s'en est aperçu tout de suite ?

ANONYME1 : Non, pas du tout... L'administrateur système n'as rien vu pendant plusieurs semaines. Nous effacions bien nos traces.

PIRAT'Z : Pas assez on dirait... ?

ANONYME1 : Nous avons laissé quelques traces pour qu'il s'aperçoive que son système avait un problème. Nous n'osions pas le voir directement par peur de représailles. Avec le recul, on se rend compte qu'on aurais dû le prévenir tout de suite.

PIRAT'Z : Quel genre de traces ?

ANONYME1 : Du genre petits mots implicites dans notre dossier personnel. On pensait que les admins vérifiaient notre espace personnel, ce qui s'est révélé vrai par la suite. C'est à partir de ce moment qu'ils ont commencé à chercher ce qu'on pouvait bien faire. On parlait aussi avec les responsables adjoints, qui sont des élèves que nous connaissions bien. On leur disait tout en pensant qu'ils balanceraient à l'administrateur. Ça ne s'est pas passé comme prévu, et ils n'ont rien dit... Ça nous aurais arrangé en fait...

PIRAT'Z : Regrettes-tu ce que tu as fait ?

ANONYME1 : Non, pas vraiment, je n'ai eu aucune autre sanction et ça m'a servi de leçon. J'aurais pu tout détruire, être un gros bourrin et faire un simple " DeL " sur les fichiers des serveurs. Je ne l'ai pas fait. J'aurais pu modifier mes notes dans certaines matières, je ne l'ai pas fait, je risquais sûrement plus d'ailleurs en faisant ça. Bref, je me suis fait choper à temps. J'ai compris qu'il faut faire plus attention et que la sécurité est à prendre au sérieux. J'ai aussi compris que le hacking, même bénin, peut-être dangereux : c'est parce que je n'ai rien fait de grave que je me suis fait prendre.

PIRAT'Z : As-tu un conseil à donner aux lecteurs de Pirat'z ?

ANONYME1 : Oui, amusez-vous, soyez curieux mais faites très attention à vous. Avant de commettre un acte dangereux, réfléchissez bien à ce que vous devez faire et l'ordre dans lequel vous le faite, après coup, c'est trop tard.

TÉLÉCHARGEZ HALO 2 SUR

PIRATZ@HOTMAIL.COM

Avec l'annonce de GMail, les fournisseurs d'emails gratuits ont (presque) tous augmenté l'espace qu'ils offrent à leurs utilisateurs. Désormais, on a bien trop d'espace ! Alors, que faire de tous ces téra-octets disponibles ? Y stocker des fichiers, bien sûr ! Mais comme le faire à la main serait assez fatigant, des logiciels commencent à apparaître pour s'en occuper automatiquement. Ainsi, RoamDrive (www.roamdrive.com) est pour l'instant compatible uniquement avec Hotmail, mais prévoit de supporter plus de webmails d'ici peu.

AVOCAT, UN MÉTIER PLEIN D'AVENIR

La MPAA (l'homologue cinématographique de la RIAA) suit les traces de la RIAA et a commencé à intenter des procès contre les internautes qui partagent des films sur Internet. Contrairement à la RIAA, elle n'a pas commencé par de simples avertissements, mais a décidé de tout de suite récolter des preuves suffisantes contre les partageurs de fichiers (les vilains) pour ensuite les poursuivre. Plus de 230 plaintes ont été portées pour commencer et plusieurs procès sont déjà en cours contre des adeptes de P2P. Le piratage de films est un fléau pour la MPAA. Non seulement les pirates partagent-ils des films déjà sortis dans les clubs vidéo, mais également des films à peine sortis en salle. Ce qui rend évidemment tous les artisans du cinéma très pauvres... Apitoyons-nous un peu sur tous les Steven Spielberg de ce monde. D'après nous, il faudra un certain temps avant que nous soyons dans la même situation, alors profitez-en, mais peut-être êtes-vous observés ! Tiens, je me demande si Overpeer ne serait pas justement en train de se construire une petite base d'IPs...

DE JUSTICE

ANONYME2 : INTRUSION SUR UN SERVEUR GOUVERNEMENTAL. PEINE: AUCUNE, INTERROGATOIRE MOUVEMENTÉ...

PIRAT'Z : Alors, raconte-nous ce que tu as fait....
ANONYME2 : Hé hé, disons que je me suis amusé avec un serveur qui appartenait au gouvernement. Au début, je cherchais des failles classiques, comme le XSS, l'SQL injection, bref, surtout des failles relatives aux scripts contenus sur le serveur. Le problème fut que leur script de recherche avait une petite faille qui m'a servi de base.

PIRAT'Z : Pourquoi as-tu subitement eu envie de chercher des failles sur leur site ?
ANONYME2 : Je bossais l'été dans une institution gouvernementale. Je m'ennuyais un peu, alors j'ai fait un p'tit tour sur leur site...

PIRAT'Z : Tu as testé ces failles au boulot ?
ANONYME2 : Non, j'ai exploité la faille du moteur de recherche depuis un cyber-café, puis j'ai réfléchi dessus chez moi. Je suis retourné au cybercafé pour essayer de voir où ça menait.

PIRAT'Z : Et comment tu t'es fait repéré ?
ANONYME2 : En fait, je me suis fait prendre à cause du mail que je leur ai envoyé pour signaler les failles... C'est con, hein ?

PIRAT'Z : Bah oué... Comment ca s'est passé ensuite ?
ANONYME2 : J'ai été interrogé, menacé. Pendant l'interrogatoire, la tension montait, mais je n'ai finalement rien eu.
PIRAT'Z : Est-ce que le fait de t'être fait intercepter alors que tu n'avais encore rien fait ne te donne pas envie de ne plus prévenir par mail lorsque tu trouves une faille ?
ANONYME2 : En effet, j'ai tendance à ne plus prévenir, mais ce n'est pas pour ça que j'utilise la ou les failles présentes sur un site. Seulement, dès que j'en vois une en .gouv.fr, je me résigne à ne plus prévenir. Ils ont des admins système compétents mais un peu violents ;)

PIRAT'Z : Est-ce que tu te considères chanceux de n'avoir rien eu ?
ANONYME2 : Un peu oui. Je connais la loi Godfrain par cœur et je savais que je risquais beaucoup, rien qu'en essayant d'exploiter des failles. Je trouve quand même dommage que de prévenir d'une faille soit répréhensible. À croire qu'ils voient ça d'un mauvais œil.

PIRAT'Z : Il faut croire que oui... Ils ont sécurisé ?
ANONYME2 : Oui, voir les gens réagir (un peu trop brusquement d'ailleurs) m'as montré que mon geste a suscité un intérêt. Il a permis au serveur d'être plus sécurisé. Je n'ose pas imaginer ce qu'un pirate au sens péjoratif du terme aurait fait à ma place. Ça me motive encore plus.

PIRAT'Z : Tu as un conseil à donner aux lecteurs de Pirat'z ?
ANONYME2 : Oui, faites attention à ce que vous faites quand vous cherchez des failles. On a vite fait de déraper, une commande de trop vous fait passer la frontière de l'illégalité. Et puis... réfléchissez avant de prévenir les administrateurs des sites par mail !

ANONYME3 : ACQUISITION ILLÉGALE D'INFORMATIONS CONFIDENTIELLES ÉTRANGÈRES. PEINE : AUCUNE [POUR LE MOMENT... ?].

PIRAT'Z : À ton tour :)
ANONYME3 : Ok, mais je vais devoir rester très vague pendant cet interview, l'histoire que j'ai vécue n'est pas terminée. J'ai téléchargé des informations confidentielles sur des travaux industriels et scientifiques d'entreprises étrangères.

PIRAT'Z : Tu savais ce que tu risquais ?
ANONYME3 : Bien sûr, je risquais la prison et une très grosse amende.

PIRAT'Z : As-tu été poursuivi ?
ANONYME3 : Non, je me suis mis directement en relation avec les services gouvernementaux français. J'ai joué un peu au chat et à la souris. J'étais en contact avec eux, mais ils ne pouvaient pas m'arrêter. Ils avaient quelque chose à gagner ...

PIRAT'Z : Peux-tu être plus précis ?
ANONYME3 : Il y avait une enquête sur moi (le contraire aurais été scandaleux). J'ai pris pas mal de contacts avec des personnes du gouvernement pour exposer ma situation. J'ai rencontré des gradés et des exécutants, les plus dangereux étant ces derniers. Ils étaient intéressés par les informations que j'avais récupérées. Au début, j'ai fait tout ça pour le fun, puis j'ai réfléchi à ce que ces informations valaient...

PIRAT'Z : Tu n'avais pas peur que le gouvernement t'arrête malgré tout ?
ANONYME3 : Je me suis d'abord retiré de la scène. J'ai stopé toutes mes activités publiques en informatique et ai cessé de faire de la sécurité ailleurs que sur mon ordinateur. Je n'ai pas repris depuis, même si j'ai des projets. J'ai bien sûr eu peur pendant toute cette période.

PIRAT'Z : Est-ce que tu avais cette petite montée d'adrénaline pendant tes rendez-vous ? ce petit jeu avec le gouvernement t'amusait-il ?
ANONYME3 : J'avais des grosses montées de stress et d'adrénaline au moment des rendez-vous physiques. Ce n'étais pas amusant, mais plutôt instructif. C'est une expérience que je ne regrette pas du tout d'avoir vécue.

PIRAT'Z : Si tu le refaisais, irais-tu encore plus loin ?
ANONYME3 : Non, juste différemment, de sorte de laisser d'autres notes dans les fichiers des services du ministère que celles qu'il doit y avoir en ce moment.

PIRAT'Z : Le commerce d'informations piratées relève du blackhat hacking. Tu te considères comme tel ?
ANONYME3 : Je n'aime pas ce manichéisme, c'est ma réponse.

PIRAT'Z : Tu as agit seul ?
ANONYME3 : J'avais des pseudo soutiens qui étaient plus dangereux qu'autre chose.

PIRAT'Z : Penses-tu moralement que tu aurais dû être arrêté ?
ANONYME3 : Avec le recul, je pense que oui. Mais dans les faits, ça aurait été une perte de temps pour tout le monde.

PIRAT'Z : Merci à tous et bonne continuation ;)

1Z

UN PIRATE BIENTÔT AUX GALÈRES

En avril 2004, l'opération FastLink, initiée par les États-Unis mais en coopération avec 11 autres pays, avait abouti à près de 100 arrestations (dont certaines en France, on a d'ailleurs perdu quelques lecteurs, comme l'ont montré nos ventes). Cette opération visait les acteurs de la Scène (les groupes Warez piratant logiciels, films, etc.). On apprend que l'une de ces personnes arrêtées, un homme de l'Iowa, est le premier à plaider coupable, et connaîtra sa sentence le 18 mars. Il risque 15 ans de prison. Je vous laisse méditer là-dessus.

KAZAA + BITTORRENT = EXEEM = ... GROSSE MERDE ?

Le site SuprNova.org a annoncé la mise à disposition sous peu d'un nouveau logiciel de P2P, eXeem, qui aurait pu devenir le nouveau Graal des amateurs de partage de fichiers. En effet, quand on entend qu'il s'agit d'un " mélange entre Kazaa et BitTorrent ", on pense " enfin on va pouvoir chercher des fichiers ". Rappelons en effet que BitTorrent ne supporte pas la recherche, ce qui contraint ses utilisateurs à trouver les liens (torrents) sur des sites web essentiellement... l'un d'eux étant d'ailleurs, jusqu'à récemment, le fameux SuprNova.org, fermé apparemment à cause de la pression grandissante de la MPAA (l'industrie cinématographique américaine) qui s'inquiète de plus en plus du téléchargement de films sur le Net. Enfin bref, si eXeem pourrait bien être dispo au moment où vous lisez ces lignes, ne vous jetez pas dessus sans réfléchir. Il semble en effet qu'outre un code propriétaire et l'absence de support de Linux et MacOS, l'aspect " Kazaa " d'eXeem signifie aussi bon nombre d'adwares et spywares bien puants. La communauté P2P est plutôt sceptique, et nous aussi !

VULNERABILITE 2004

Quand on prend le temps de passer en revues toutes les vulnérabilités qui ont été découvertes et annoncées l'année dernière, ça fait peur. Voici une petite sélection, toute subjective.

IE A LE FEU AU CUL

Pour ceux qui, comme moi, désespéraient de trouver une alternative correcte à Internet Explorer, Firefox s'avère la solution idéale. La version 1.0, maintenant disponible sur getfirefox.com, est compatible avec Windows, Linux, MacOS, ne déroute pas l'utilisateur familier d'IE, offre un système de skins vraiment cool, et surtout plein de plugins (extensions) très utiles. Notamment AdBlock, pour éliminer les publicités présentes dans les pages web. Enfin le concurrent sérieux à IE que l'on attendait, depuis la déroute de Netscape.

WPA : FIN DU MYTHE

À votre plus grand désespoir vous ne pouviez plus utilisez la connexion wifi de votre voisine. Impossible de récupérer ses photos en tenue légère sur son partage. La faute à qui ? WPA : votre pire cauchemar ! En effet, le temps où vous crackiez sa clef wep 68 bit après trois semaines de sniff et un mois de brute force est bien révolu... Pour ceux qui ne savent pas de quoi on parle, la clef wpa est la nouvelle génération de clefs qui permet de sécuriser (pas complètement) ses connexions wifi. Celle-ci remplace désormais les clefs wep bien trop sensibles au brute-force.

Mais arrêtez de vous morfondre car une clef wpa peut enfin être cassée simplement. Pour ce faire, il suffit d'utiliser le logiciel wpa-crack. Ne paniquez pas non plus, car seules les clefs courtes ou contenant des mots usuels sont facilement crackables. Comme toujours, plus le pass est complexe, plus vous compliquerez les choses. Privilégiez donc des mots de pass longs (plus de 20 est recommandé pour une clef wpa), n'utilisez pas de mots du dictionnaire et pensez aux caractères spéciaux ;)

LINUX 2.4.24/2.6.2 DO_MREMAP II

CVE-2004-0077

Voilà une nouvelle vulnérabilité kernel découverte dans Linux. Des failles dans les appels système do_brk et do_mremap, avaient déjà été publiées l'année précédente. Sans rentrer dans les détails, ces appels servent à gérer la mémoire des processus. Ici, do_mremap ne vérifie pas un message d'erreur renvoyé par une fonction qu'il utilise. Cette erreur ne se produit normalement pas, sauf dans des conditions spéciales, dans lesquelles on peut alors tromper do_mremap et, par exemple, faire exécuter du code à un programme privilégié - ce qui mène à obtenir les droit de root.

Solution : mettre à jour le noyau.

*BSD SHMAT[]

CVE-2004-0114

Encore un problème kernel, dans BSD cette fois (FreeBSD <= 5.2, NetBSD <= 1.3, OpenBSD <= 2.6), en rapport avec la gestion de la mémoire partagée. Ce bug permet d'avoir accès en lecture et écriture à une portion de la mémoire kernel. Cette partie de la mémoire n'est normalement pas accessible aux utilisateurs, parce qu'elle contient des informations critiques, donc certaines permettent d'élever son niveau de privilèges. Cette vulnérabilité permet donc de passer root.

Solution : mettre à jour le noyau.

WINDOWS LSASS REMOTE BUFFER OVERFLOW

CAN-2003-0533

Cette faille, rendue célèbre par le vers Sasser, a été découverte fin 2003, mais publiée en avril 2004. Il s'agit d'un classique buffer overflow dans le tas, qui permet de prendre le contrôle à distance de Windows NT 4, 2k SP2, XP SP1, et Server 2003, autrement dit d'un paquet d'ordinateurs dans le monde entier, en tout cas à l'époque. Ça fait mal !

Solution : MS04-011 / XP ServicePack2

WINDOWS CHM HEAP OVERFLOW

CAN-2004-0201

Un buffer overflow peut être produit et exploité à partir d'un fichier d'aide .chm, sur Windows 98, Me, NT 4.0, 2000, XP et Server 2003. Un pirate s'arrangerait donc pour que sa victime ouvre un fichier d'aide préparé pour exploiter la faille, ce qui peut se faire automatiquement en utilisant certaines failles d'Internet Explorer.

Solution : WindowsUpdate.

TCP LARGE WINDOW SEQUENCE NUMBER PREDICTION

CAN-2004-0230

Il ne s'agit pas réellement d'une vulnérabilité, mais d'une faiblesse inhérente au protocole TCP/IP. Vous savez que les connexions réseau sont faites avec des paquets qui sont routés à travers l'Internet. A priori, on pourrait créer de faux paquets, afin d'injecter ce que l'on veut dans une connexion existante, ou balancer un faux paquet pour la couper. Cependant, il est difficile de le faire en aveugle avec des connexions TCP, parce que ce protocole utilise des numéros de séquences, qu'il est difficile à prévoir. Si on n'a pas le bon numéro, les paquets injectés seront simplement ignorés. Théoriquement, on a une chance sur 4 milliards de trouver le bon numéro de séquence, c'est pas gagné d'avance. Cependant l'attention du public a été portée sur le fait qu'un paquet était pris en compte lorsque son numéro de séquence était inclus dans un intervalle dépendant de la fenêtre TCP en cours, qui détermine justement combien de paquets le destinataire est en mesure de recevoir à l'avance. Comme la valeur de cette fenêtre varie généralement entre quelques milliers et quelques dizaines de milliers, on a beaucoup plus de chance, en fait, de tomber sur un numéro de séquence valide.

Solution : aucune.

CPANEL / MOD_PHPSUEXEC /SUEXEC

CAN-2004-0490, CAN-2004-0529

cPanel est une application commerciale, basée sur des logiciels libres, utilisée pour la gestion d'hébergement mutualisé par beaucoup de sociétés de webhosting. Plusieurs vulnérabilités ont été découvertes dans ce système cette année, corrigées maintenant. Il y a d'abord un problème avec la version de mod_phpsuexec, tel qu'il était compilé par cPanel. Ce module apache permet d'exécuter des scripts PHP avec des droits différents selon le site (normalement, tous les scripts php du serveur sont exécutés en tant qu'un utilisateur commun, unique et non privilégié, comme nobody ou www-data, ce qui ne convient pas pour du multi-hosting). Un problème de chemin permettait cependant à un client d'exécuter un script de son choix avec les droits d'un autre utilisateur.

À cause d'une modification apportée par cPanel à suexec, qui sert à exécuter les scripts CGI, cette fois, avec les bons privilèges, un utilisateur local pouvait aussi détourner l'exécution de certains scripts qu'il faisait exécuter par root. Il n'est plus possible d'utiliser suexec pour faire exécuter ces scripts en tant que root, dans la version actuelle, mais certains (notamment proftpdvhosts) pourraient toujours être détournés, si jamais un autre problème similaire était découvert.

On peut se demander toutefois pourquoi un client voudrait pirater son propre hébergeur. Mais la question n'est justement pas là, vu qu'un pirate pourrait tout à fait prendre le contrôle du compte de quelqu'un, en passant par une faille php de l'un des sites hébergés.

Solution : http://www.cpanel.net

WINS REMOTE CODE EXECUTIONS

CAN-2004-0567, CAN-2004-1080

WINS sert à la résolution de noms pour les accès NetBIOS, et évite notamment d'avoir à faire des broadcast pour trouver une machine dont on ne connaît que le nom (ça ressemble aux DNS). Deux problèmes différents ont été découverts dans ces services, qui semblent tous deux permettre l'exécution de code à distance. Les détails n'ont pas encore été rendus publics au moment de la rédaction de ces pages, mais un correctif est déjà disponible. Espérons qu'on aura pas droit à un nouveau vers...

Solution : Désactiver WINS / MS04-045 / XP SP2

PHPBB2/HIGHLIGHT

CAN-2004-1315

Une vulnérabilité critique a été découverte dans phpBB 2.0.10 et inférieur, qui permet d'exécuter du code php à travers l'option highlight (mise en évidence de mots clés). C'est assez grave, vu que phpBB2 est très populaire, et que l'exécution de code php permet à un pirate de presque tout faire. Heureusement - du moins c'est un point de vue - un vers se propage via cette vulnérabilité, en trouvant ses victimes avec Google. Du coup, les gens risquent de mettre leurs forums à jour rapidement.

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 / LOGPIRAT'Z

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 : .....

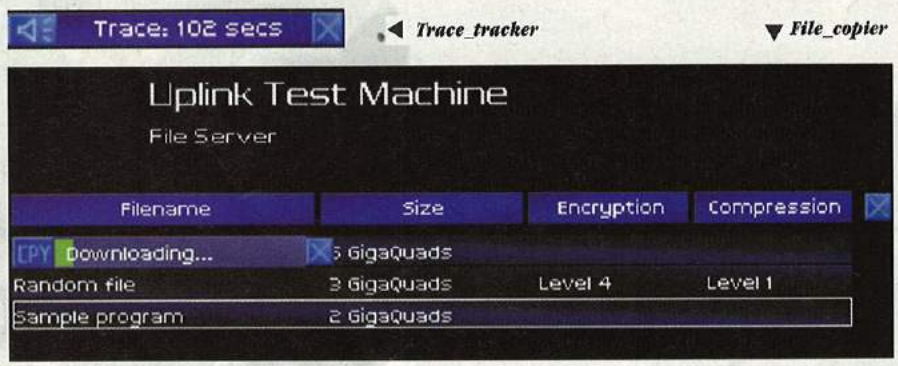
☐ Chèque à l'ordre de PUBLIA

☐ Mandat à l'ordre de PUBLIA

Signature

HACKEZ LA CIA AVEC UPLINK

Si vous ne connaissez pas déjà ce jeu sur le thème du hacking, vous allez adorer : toute l'excitation de pirater des systèmes, sans les risques, et sans s'embêter à lire et comprendre des tas de trucs techniques.



À Pirat'z, on aime le GUI-hacking, surtout quand c'est pour de faux. Vous avez déjà tous vu des films, ou surtout tant de séries télé, avec des scènes de piratage exceptionnelles et des interfaces 3D pleines de couleurs. Le plus drôle, c'est qu'il semble que plus le "hacker" tape vite au clavier, plus il a de chances de réussir. Depuis le temps que vous lisez le mag, vous savez que c'est un poil exagéré, pas vrai ?

Il existe encore pas mal d'outils pour script-kiddie qui permettent de lancer un exploit en deux ou trois clics ou de scanner un class B sans les mains. Mais ça, c'est de la rigolade. C'est vrai aussi que les professionnels du hacking légal, ceux qui font des tests d'intrusion pour des sociétés, en ont tellement marre de faire toujours la même chose qu'ils commencent à se développer des outils sympas, automatisés, avec des interfaces graphiques et tout. Et en plus, ils vendent généralement ça très cher, on se demande à qui : $1000 pour CANVAS, sur http://www.immunitysec.com ...

Il faut pourtant se rendre compte que le hacking hardcore, ça ne se pratique pas vraiment avec ce genre de jouets. Il s'agit plutôt de maîtriser la ligne de commande, ne pas avoir peur de sortir son compilateur C au moment opportun, et savoir composer avec les outils existants et ceux que l'on va se créer. Un exemple étonnant de cela se trouve dans Matrix Reloaded, l'exception à la règle, où l'on voit Trinity utiliser nmap (http://www.insecure.org) pour scanner sa cible, avant de lancer un bon vieil exploit de 2001 (un bug dans l'implémentation de ssh1) pour réinitialiser le mot de passe root à distance.

Si le GUI-hacking n'a que peu de charme en matière de réalisme, on ne peut pas dire que ce ne soit pas tripant. C'est ce qu'a compris Introversion, une société anglaise qui fait des jeux vidéo indépendants, en proposant avec Uplink un concept vraiment réussi et accrocheur, tiré du thème du piratage. C'est vrai que c'est un jeu qui date de début 2001. Mais quand on n'a pas de trucs alléchants à mettre sur la couverture du mag, faut bien faire les fonds de tiroirs... Et puis, en vérité, je ne l'ai découvert qu'il y a très peu de temps, vu que jusqu'à présent je ne pouvais pas faire fonctionner l'accélération graphique sur mon Linux. Donc pas moyen d'y jouer. Je sais, ça tourne aussi sur Mac et Windows. Mais faute d'excuse plus convaincante, je me dis que quelques-uns d'entre vous n'en ont jamais entendu parler. Et il est peut-être temps pour les autres de s'y remettre (voir l'encadré sur Onlink) !

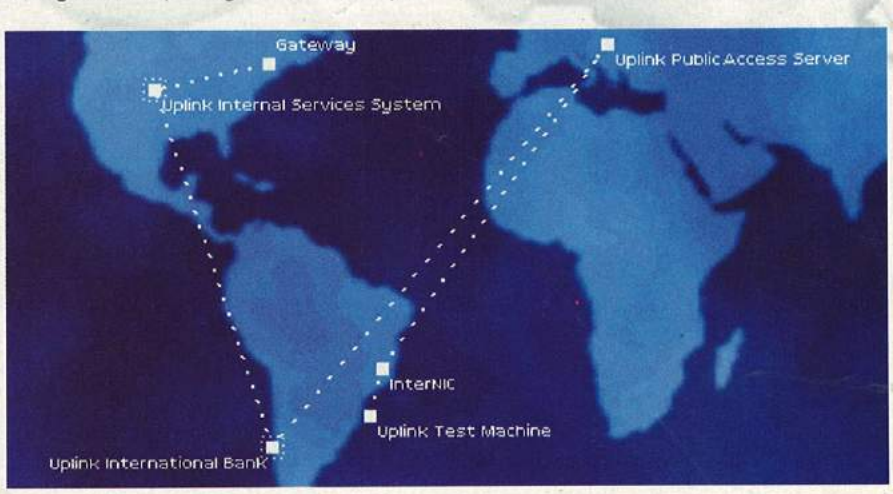
LE JEU

L'action se passe en 2010, dans un contexte très high-tech d'espionnage industriel et de piratage informatique. Vous incarnez un agent d'Uplink, un genre de hacker qui pénètre les systèmes à la solde de grosses sociétés. Votre but est de tirer un max de thunes de ce savoir faire.

Uplink, c'est un peu l'agence d'interim du cybercrime, dans l'histoire, c'est l'intermédiaire entre vos futurs clients et vous, et il vous loue en passant une connexion et une passerelle relativement anonyme. En se connectant sur le serveur de l'organisation, vous avez accès à une série de services. Vous pouvez notamment mettre à jour votre arsenal hardware et surtout software (des crackers, scanners, log cleaners, et autres outils anti-sécurité). On y trouve aussi un BBS où sont publiées des offres de travail pas très catholiques.

Les missions qu'on vous propose sont sympathiques : sabotage, espionnage industriel, falsification d'informations personnelles, etc. En pratique, elles consistent à se connecter sur la cible, à y voler un accès, si possible d'administrateur (avec un cracker de mot de passe, par exemple), faire ses viles affaires, et enfin effacer ses traces. Mais ce qui fait monter l'adrénaline dans tout ça, c'est que dès le premier faux-pas, vous êtes traqué. Les gens que vous attaquez tentent de vous tracer, et vous avez donc très peu de temps pour faire le sale boulot.

Si vous ne vous êtes pas déconnecté à temps ou que vous n'avez pas pu effacer correctement les traces qui pourraient trahir votre identité, vous risquez au mieux une amende, au pire de vous faire arrêter, et donc de perdre le jeu parce qu'Uplink vous aura lâchement dénigré. C'est pour cela que vous devez brouiller les pistes en passant par autant d'intermédiaires que vous pourrez. Si



pour atteindre votre cible, vous passez par exemple par une machine déjà compromise et dont vous êtes maître, la tâche sera plus difficile pour ceux qui vous traquent. Idem si vous passez par une machine appartenant à l'État ou par une banque, vu qu'il est plus difficile d'obtenir des logs de ces systèmes. Vous gagnerez ainsi quelques secondes précieuses.

Pour réussir la mission de test par laquelle commence le jeu, achetez un Dictionary_hacker, et un Trace_tracker (la v3 vous indique combien de temps il vous reste avant d'être pris, pratique) avant de vous connecter à la machine.

Et pour le reste, bonne découverte, et bon GUI-hacking ;-)

INTROVERSION

Au delà de son excellent gameplay, Uplink est aussi la preuve qu'on peut développer un jeu original tout seul dans sa chambre et le vendre. Enfin presque. Le jeu a été créé par un petit groupe de développeurs, sans locaux, et surtout sans la pression d'un responsable vente-marketing qui leur imposerait des contraintes absurdes. Leur succès - tout relatif, bien sûr, si l'on considère les ventes insultantes des multinationales du jeu vidéo - ne vient pour une fois que de la qualité du jeu, et non de campagnes de publicité. Leur but : faire bouger l'industrie du jeu et proposer au public des idées vraiment novatrices. Voyez ce que ça donne après Uplink, si vous avez la chance de participer au betatest de leur prochain titre, Darwinia.

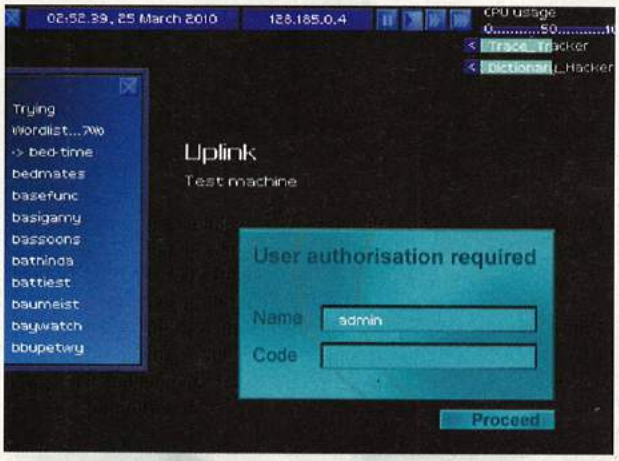
Si vous avez finalement décidé d'acheter un jeu au moins une fois dans votre vie, ce sont les bonnes personnes, conseil de Pirat'z !

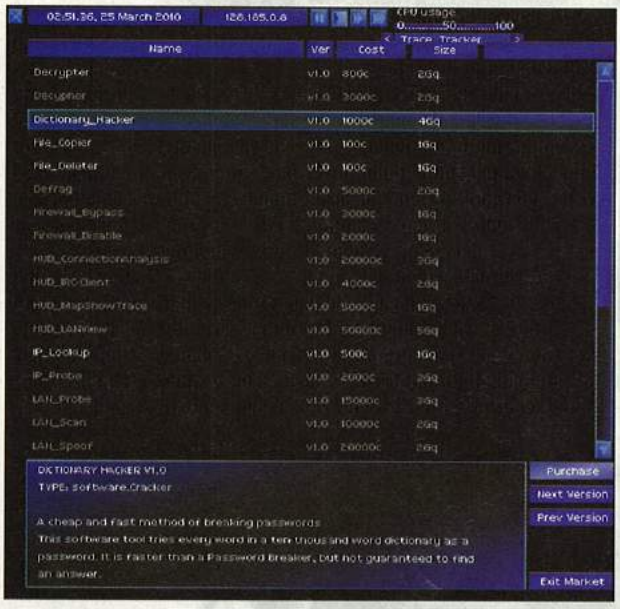
de Bazande

On peut télécharger la démo sur : http://www.uplink.co.uk/

La version complète coûte dans les 34 euros tout compris.

Leur prochain jeu : http://www.darwinia.co.uk/





Upgradez votre système

ONLINK, UN MOD DISPONIBLE EN FÉVRIER 2005

Vous avez terminé la démo, acheté le jeu complet, que vous avez terminé aussi ? Vous en voulez encore ? Tout n'est pas perdu. Les créateurs d'Uplink ont eu le bon goût de laisser une porte ouverte aux autres développeurs qui voudraient contribuer à prolonger la durée de vie du bazar. Il est donc possible de concevoir de nouveaux scénarios, d'ajouter des options, des dispositifs, du software, du hardware, tout ce que l'on veut. C'est ce qu'une équipe de passionnés a fait, ou du moins achève de faire, avec Onlink.

Plus parlant qu'autre chose, voici une rapide interview réalisée sur le serveur IRC du jeu.

baze : Est-ce que tu peux me parler de l'équipe ? Vous êtes tous des fans frustrés d'avoir terminé le jeu trop vite ?
Riddla : Nous étions environ six au commencement, dont quatre coders, un webmaster, et moi, le scénariste. Nous nous sommes rapidement retrouvés deux ou trois. Il y a Kyuuketsuki, le leader du projet et programmeur principal, NeoThermic, notre expert en sécurité (qui s'assure qu'on ne fait pas tout de travers ;o) et moi.
baze : Peux-tu nous révéler quelques éléments exclusifs du nouveau scénario ?
Riddla : Haha ! Aucune chance, mon ami :)
baze : Allez, juste un ou deux trucs...
Riddla : Bon, tout ce que je dirai, c'est que l'histoire se passe 10 ans après celle de l'original. Une grande partie des dégâts causés par *revelation* ont été réparés, et de nouvelles technologies émergent. En fait, le monde est plus dépendant de la technologie que jamais.
Et voilà :P
baze : À quoi va servir ce nouveau software (parmi des dizaines d'autres) : *Console Inject* ?
Riddla : Gosh, il faut que je rassemble mes notes ;o
Le *Console Inject* te sert lorsque tu as besoin d'un accès console à une machine qui n'a justement pas de console. C'est un peu comme installer DOS avec une disquette, mais à distance. Tu peux imaginer des systèmes haute-sécurité qui n'auraient pas de consoles pour des raisons de sécurité.
Toutes les idées en rapport à la sécurité viennent de Kyuuketsuki. J'ai juste comblé les blancs.
baze : Des attaques par sociale engineering, c'est prévu ?
Riddla : L'interaction entre les personnages, dans Uplink, ne va pas si loin. Nous avons ajouté la possibilité de pirater les ordinateurs personnels pour récolter des informations, mais je ne crois pas que Uplink soit vraiment adapté pour ce genre de choses. Il a été conçu pour simuler du hacking hi-tech.
baze : Et qu'est-ce qui va sortir exactement en février ?
Riddla: Il est prévu de distribuer Onlink en cinq étapes. Kyuu a codé un système de mise à jour automatique, ainsi le jeu se patchera lui-même sans avoir à télécharger de nouvelles versions sur le site. En février, j'espère que toutes les nouvelles technologies seront disponibles, ainsi que le scénario. Mais nous allons nous concentrer avant tout sur la finalisation d'une version qui marche.
baze : Merci beaucoup ! Est-ce que tu as quelque chose à ajouter ?
Riddla : Seulement que nous savons que c'est une projet ambitieux, mais que nous avons travaillé dur depuis onze mois déjà, et que nous espérons terminer tout ce que nous avons prévu.

Avis aux anglophobes : un certain Mafio24 travaille sur une traduction française d'Uplink, et a été contacté par l'équipe d'Onlink.

http://www.neothermic.com/onlink/

XBOX : LES SECRETS DE LA BOITE NOIRE

Tout ce que vous aviez toujours voulu faire avec votre XBOX, mais que vous n'étiez pas sensé faire. Avant de faire passer un PC presque donné pour une console de luxe, Bill Gates aurait mieux fait de réfléchir.

1ÈRE PARTIE

Désireux de s'imposer dans le monde du jeu vidéo sur console, Microsoft a créé la XBOX. Alliant toutes les qualités d'un PC à la facilité d'utilisation d'une console, elle est le "Multimedia Center" idéal. Les hackers passionnés découvrant peu à peu les secrets de cette boîte noire nous permettent aujourd'hui d'utiliser cette console au delà de ses fonctions d'origines. Jeux, DVD, MP3, DivX, Radios & TV internet, Emulateurs, et même Linux, pour la transformer en véritable PC.

Cette inspiration de concepts propres au monde PC se retrouve directement dans le hardware de la console. La partie matérielle de la XBOX est composée d'éléments de PC, ce qui facilite les modifications.

Le travail des hackers fut activé par la récompense promise au premier arrivant a lancer Linux sans modification matérielle. Cette technique a évolué en plusieurs exploits utilisant les failles des jeux et du système d'exploitation pour permettre de lancer des copies de jeux et programmes non officielles. Toutes ces techniques permettent aujourd'hui de profiter de tous les avantages d'une puce (également appelée modchip) sans en avoir, ce qui permet de faire quelques économies.

LE HARDWARE DE LA CONSOLE

Avant d'entrer dans le vif du sujet, nous allons nous intéresser au matériel de la XBOX et à la manière de la démonter.

Pour démonter une XBOX, il faut se munir d'un tournevis Torx 20 pour les vis extérieures, et Torx 10 pour l'intérieur.

Retournez la console et dévissez les six vis : Il y a une vis sous chaque étiquette, et une vis cachée sous chaque patin (entourés en jaune). Enlevez toutes les vis et retournez la console à l'endroit. Otez le capot, vous voyez maintenant le lecteur DVD et le disque dur. Si vous avez une XBOX de première génération (v1.0) votre disque dur est de 8 Go, pour les plus récentes c'est un 10 Go.

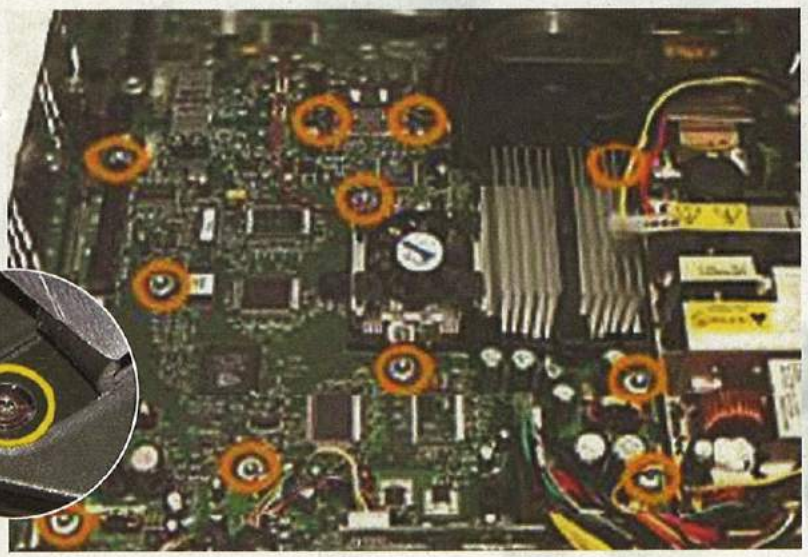
Débranchez la nappe IDE et le câble d'alimentation du disque dur.

Dévissez les vis indiquées par les points rouges. Vous pouvez ensuite enlever le disque dur. Débranchez la nappe et les fils jaunes du lecteur DVD, puis enlevez-le.

près ;-) On voit ici que c'est une carte mère de XBOX Version 1.0, notamment grâce à la présence d'un petit ventilateur sur le GPU. Les XBOX de version supérieure à la 1.1 n'en sont pas équipées.

En effet, toutes les XBOX ne sont pas identiques. De la v1.0 à la v1.6, il y a quelques changements.

- Disque Dur : 8 Go Western Digital (1.0) ou 10 Go Seagate (>1.0)
- Lecteur DVD : Thomson, Philips, ou Samsung (les Zamsung lisent plus facilement les CD-R)
- Ventilateur GPU présent (1.0) ou absent (>1.0)
- Câblage du panneau avant par un ci amovible (1.0) ou intégré à la carte mère (>1.0)
- Alimentation : Connecteur Type AT (1.0 et 1.1) ou Type ATX (>1.1)
- Encodeur vidéo : Conexant (1.0-1.1), Focus (1.1-1.4), et même Xcalibur (1.6), le Focus a posé quelques problèmes pour certains exploits, mais c'est maintenant résolu grâce aux nouveaux bios compatibles avec toutes les versions.



Vous avez devant vous la carte mère ainsi que l'alimentation de la XBOX.

Vous pouvez maintenant dévisser les onze vis de la carte mère si vous voulez l'examiner de plus

- TSOP : 1 Mo (1.0-1.1) ou 256 Ko (1.1-1.4) e sur la 1.6 remplacé par le Xyclops : un compo sant regroupant plusieurs fonctions.

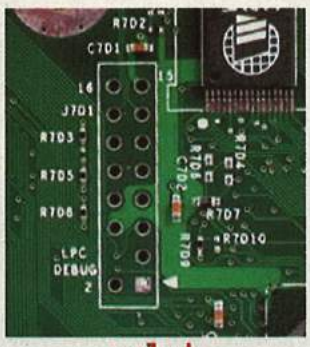
ATTENTION

Le fait de dévisser rien qu'une seule vis de votre console XBOX entraînera la perte de la garantie, ce qui peut être assez ennuyeux si vous venez de l'acheter. Si la garantie de votre console est dépassée, alors vous pouvez la démonter avec un peu plus d'assurance, mais il faut savoir qu'en cas de panne, votre console ne pourra pas être réparée par Microsoft :-(De plus, toute reproduction autre que l'établissement d'une copie de sauvegarde par l'utilisateur est illicite. En clair, n'utilisez pas les méthodes que vous allez apprendre pour jouer à des jeux que vous n'avez pas achetés. Vous voilà prévenus ;-

Chaque manette est un HUB, car les deux slots pour cartes mémoires sont aussi en USB. Cela permet de se servir de la manette pour installer un port usb à la place d'un slot pour carte mémoire.

Le disque dur et le lecteur DVD sont aussi des éléments de PC. Le DVD a une prise d'alimentation différente, mais le disque dur est identique à celui d'un PC et on peut le changer, mais pas n'importe comment car il est protégé par un mot de passe unique correspondant à la console. Nous verrons dans un prochain article comment procéder.

v1.6



v1.4

Le flash du TSOP n'est pour le moment possible que sur les versions inférieures à la 1.6, car le Xyclops n'est pas un composant standard.

Pour identifier une XBOX à coup sûr, on peut utiliser le programme XBOX Version Detector, qui peut être lancé directement par un exploit.

LA XBOX EST UN VÉRITABLE PC

- Processeur Intel Celeron 733Mhz,
- Processeur graphique équivalent à une GeForce3 MX,
- 64 Mo de RAM,
- Disque dur de 8 ou 10 Go,
- Lecteur DVD,
- Réseau Ethernet 10/100.

Les ports manettes de la XBOX sont en réalité de simples ports USB, seule la forme de la prise est différente et un câble supplémentaire a été ajouté. On peut facilement fabriquer soi-même des adaptateurs USB/XBOX pour brancher clavier et souris USB, ce qui est très utile pour Linux.

Il suffit de dénuder un câble de rallonge pour manette XBOX et de relier un à un les fils à une prise USB standard (en suivant les couleurs indiquées sur les schémas) pour fabriquer un câble qui permet de relier n'importe quel périphérique USB standard à la XBOX. L'opération inverse peut aussi être réalisée pour connecter une manette XBOX à un PC.

Le TSOP de la XBOX est un composant interne où est stocké le BIOS, c'est ce qui gère les fonctions essentielles de la console dès le démarrage (avant même le disque dur). C'est aussi le BIOS qui contrôle si un jeu ou un programme peut être lancé (impossible de lancer un jeu gravé). Le but des modifications permettant de lancer des jeux gravés est de remplacer, modifier, ou émuler le BIOS pour que la console accepte de lancer tous les fichiers.

LES DIFFÉRENTS MODS

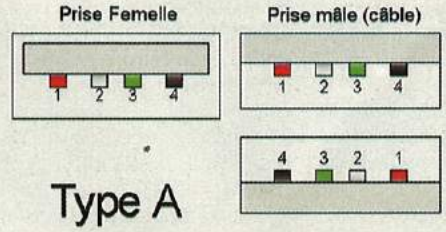
Il existe plusieurs méthodes pour modifier une XBOX, certaines nécessitant des opérations sur le matériel (ce qui implique une perte de la garantie).

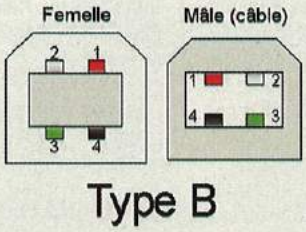
La méthode la plus connue est la pose d'une puce, que l'on soude sur le port LPC de la console. Le BIOS de la puce vient alors remplacer le TSOP de la console.

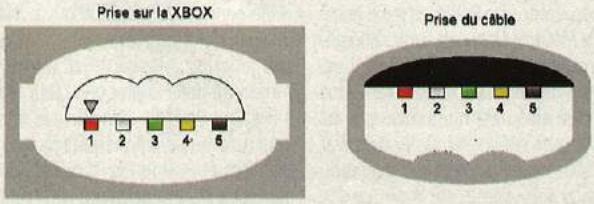
Une nouvelle méthode consiste à exploiter les failles (défauts de programmation bien connus des hackers) du système d'exploitation de la XBOX (Dashboard Microsoft).

Pour simplifier la chose : grâce à des fichiers de police de caractère trop grands, cela provoque un buffer overflow (dépassement de tampon) permettant d'exécuter du code arbitraire, c'est-à-dire n'importe quel programme.

Une autre méthode consiste à exploiter les failles dans certains jeux comme : 007, Mechassault, ou Splinter Cell.







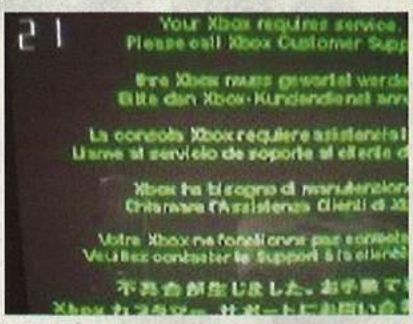
Des exploits utilisant des sauvegardes de jeux modifiées dans le but d'exploiter ces failles ont été codés, ce qui va nous rendre la tâche beaucoup plus simple et accessible à tous.

Ces exploits ont un but commun : le lancement d'un programme. Ce peut être un programme qui va flasher le TSOP de la console avec un BIOS hacké permettant de lire les jeux gravés, et d'utiliser un autre Dashboard que celui de Microsoft. Si vous n'avez pas du tout envie d'ouvrir votre console et de faire quelques soudures, vous pouvez utiliser l'exploit des sauvegardes de jeu, qui lancera un programme pour émuler un BIOS à chaque démarrage.

Chaque exploit a ses avantages et ses inconvénients, mais le principal avantage commun à ces exploits est qu'il est possible de lancer les copies de jeux comme si une puce était installée, ce qui permet de faire quelques backups. Cependant ces exploits n'offrent pas toutes les possibilités des puces de dernière génération, mais je pense que c'est déjà bien satisfaisant pour une méthode qui ne coûte (presque) rien (il faut tout de même avoir le jeu).

Après cette partie théorique, je pense que la plupart d'entre vous ont envie de passer à la pratique. Sachez que pour chacune de ces méthodes, même si les manipulations sont très simples en elles-mêmes, il vous faudra être patient, minutieux, et faire attention lors de manœuvres délicates pour ne pas endommager votre matériel car jouer avec le BIOS reste tout de même assez dangereux.

Si malgré tous ces conseils vous obtenez ce type d'écran :



C'est que vous avez probablement fait quelque chose qui n'a pas plu à votre console ;-)

Dans les prochains articles, je vais expliquer en détail comment utiliser ces exploits pour vous permettre (enfin) de pouvoir jouer à vos copies de jeu sans puce et ainsi apprécier les capacités multimédia de cette console pour lire DVD et DivX ou bien y installer Linux presque aussi simplement que sur un PC. Sans oublier la découverte des failles du Xbox live pouvant permettre à un pirate de jouer sans payer, alala on n'est pas sérieux chez Microsoft ;-)

N@k

HDLOADER LA RE

Ce Hdloader, qui permet de jouer à partir d'un disque dur, est tellement génial qu'il a été interdit de vente. Mais si on ne peut plus l'acheter en France, rien n'empêche d'en décrire toutes les possibilités...

NOËL POUR TOUS ?

Comme vous avez pu le constater, Noël ne s'est pas exactement déroulé comme prévu. En effet, une quantité astronomique de cadeaux n'a pas été livrée aux bons endroits ! Certains auraient pu penser à l'action d'un père fouettard en reste, qui comme chacun le sait, sévit toujours à cette période. Et pourtant il n'en est rien... La faute à qui, me direz-vous ? Il semble que le, ou plutôt les responsables, soient un groupe de terroristes proche de Ben Laden qui, en réaction à cette fête païenne, aurait piraté et modifié le contenu du serveur de commande du père Noël.

POURRITURE EN VERLAN ?

Eh oui, ça faisait longtemps que nous ne vous avions pas parlé de Retspan ! Nous allons tout de suite remédier à ce grave manquement. Il est bien sûr de notre devoir journalistique (journaliste, ça ne rigole plus ;)) de rappeler les abus que commet cette association, hélas toujours active, dont les méthodes ne sont pas sans rappeler celles d'un ancien régime. Mais Retspan, c'est quoi ? Eh bien, c'est à la base une bande d'étudiants partie en croisade contre une France à la dérive, ne faisant plus usage de sa connexion internet que pour télécharger sur le p2p le dernier album de Céline Dion (à la dérive pour le p2p, pas pour Céline Dion vous l'aurez compris) ! Cette petite milice du Net a donc décidé de protéger les pauvres majors qui, il faut le dire, en avaient grandement besoin. Leurs méthodes en revanche ne prêtent pas à sourire : menace, incitation à la délation, délation, rumeurs, mensonges avérés. Cette association d'un pathétique sans limite sévit toujours. Je vous invite donc à vous documenter, et même à vous insurger. Napster est mort, à quand retspan ?

Pour jouer avec des copies de sauvegarde à partir d'une Ps2 et sans mettre de puce, il y avait le " Swap Magic " pour les jeux Ps2 et le " Breaker Pro " pour les jeux Playstation. Mais ce n'est pas vraiment le remède miracle et cette méthode est loin de donner les mêmes résultats qu'une puce.
Sony avait prévu l'emplacement d'un disque dur, mais jusque-là, qui en a vraiment profité ? C'est là qu'intervient HDloader en créant ce qui va révolutionner le monde de la Ps2 ! Efficace aussi bien avec que sans puce.

Matériel nécessaire : HDloader, adaptateur modem Sony, disque dur Sony ou à la norme IDE de 40Go à 120Go et, bien sûr, une Ps2.

PS2 SANS PUCE

Pour pouvoir mettre le disque dur sur la Ps2, il faut obligatoirement acheter l'adaptateur modem, qui permet d'insérer un disque dur dans la baie prévue à cet effet. Attention, si vous mettez un disque dur non compatible, votre adaptateur modem ne pourra plus être utilisé avec un HDloader (nous vous invitons à visiter http://hdloader.xavboxps2.com afin de voir si une technique a été trouvée entre temps, pour pouvoir le réinitialiser; nous en reparlerons bien sûr dans les prochains Pirat'z). Certaines boutiques vendaient le pack complet HDloader/Modem adaptateur/Disque dur, ceci évitant tout conflit de compatibilité.

Mode d'emploi :

1 - Connecter le disque dur au modem adaptateur de Sony, puis le mettre dans le logement prévu à cet effet (une seule vis pour le maintenir, pas besoin d'ouvrir la console, on ne perd donc pas la garantie Sony).

2 - Brancher la PS2 et insérer le disque HDloader comme si on mettait un jeu. Au premier démarrage, le menu indique que le disque dur doit être formaté, ce que vous faites. Vous découvrez alors une interface simple et intuitive tout en français [ouf :-)]. Seulement, quatre menus : jouer / installer / supprimer / renommer /ainsi que la taille du disque dur et l'espace libre disponible sur celui-ci.

3 - Prendre un jeu et, à l'aide du soft (cliquer sur " installer "), le copier sur le disque dur de la Ps2. Attention, cela prend entre 20 et 30 mn pour un jeu de 4Go (à cause de la vitesse de lecture du lecteur DVD de la Ps2). Petite erreur lors de la traduction du soft en français, il faut sélectionner " supr " au lieu de " fin " une fois que le jeu est nommé.

4 - Il suffit enfin de choisir " jouer " pour lancer le jeu se trouvant sur le disque dur.

RAPPEL IMPORTANT
Le HDloader n'a pas pour but d'inciter au piratage. Pour rester en accord avec la législation en vigueur, vous devez posséder les originaux des jeux que vous mettez sur le disque dur. Le piratage a une incidence directe sur le prix de vente des jeux.
Un mois après sa sortie, HDloader à été retiré de la vente à la demande de Sony (cinq boutiques françaises ont été assignées devant les tribunaux parce qu'elles vendaient ce produit). Bien que relaxées, on ne peut plus acheter le HDloader en France. Vous pourrez suivre toute l'actualité du HDloader sur http://hdloader.xavboxps2.com.

PS2 AVEC UNE PUCE

Le principe est le même, donc quel est l'intérêt d'avoir le HDloader quand une puce est déjà installée dans sa console ? Cela permet tout simplement de pouvoir lancer les jeux directement de la Ps2 sans avoir à mettre le CD ou le DVD : le chargement des jeux est plus rapide, on n'use donc pas le bloc optique de la Ps2, et on peut aller jouer chez un pote sans avoir à prendre une brouette chargée de jeux !

Jeux incompatibles avec HDloader
- **Amplitude**
- **ATV Quad Power Racing 2**
- **Karaoké Révolution**
- **MLB 2005**
- **MX 2002: Featuring Ricky Carmichael**
- **Peter Pan: The Legend of Neverland**
- **Ratchet & Clank**
- **Samurai Warriors**
- **Soul Calibur 2**
- **Spyro: Enter the Dragonfly**
- **Tom Clancy's Rainbow Six 3**
- **Tom Clancy's Splinter Cell: Pandora Tomorrow**

Si vous en trouvez d'autres, merci de le signaler sur le site officiel ou sur le forum de Pirat'z (www.piratz.fr.st).

TEST DU HDLOADER

J'ai donc essayé le HDloader avec une Ps2 sans puce, et avec une Ps2 avec puce (testé avec puce Matrix Infinity). La seule différence, c'est qu'avec une Ps2 modifiée, il est possible de mettre la copie d'un jeu. Vous comprendrez aisément que nous ne nous attarderons pas sur ce point, car bien évidement vous devez posséder l'original du jeu que vous sauvegardez sur le disque dur.

Avec un disque dur Maxtor 120Go neuf, aucun problème : le disque dur est formaté très rapidement et tout de suite prêt à être utilisé dans la console. On peut prendre le HDloader avec l'adaptateur modem et le disque dur, et jouer avec sur une autre Ps2 (contrairement à la Xbox, le disque dur n'est pas locké : un disque dur locké ne peut pas être utilisé sans son code, il est donc inutilisable en dehors de la console dans laquelle il a été locké).
J'ai ensuite pris un disque dur de 250Go de ma Xbox pour l'essayer sur la Ps2. Je vous déconseille ce genre de test, que le modem semble d'ailleurs ne pas supporter ; il devient inutilisable avec le HDloader, même dans une autre Ps2 (les fonctions modem sont OK, mais pour le HDloader, c'est mort).

Quelles sont les différences avec les autres produits ne nécessitant pas de puce ?

Le Swap Magic est un soft qui permet de lire des copies de sauvegarde de jeux (sous forme de CD ou de DVD, selon la version du Swap Magic installée). Il faut démonter la face avant du tiroir d'éjection, on force le mécanisme de la Playstation2 à chaque utilisation du " Slide Card " (petite patte en plastique servant à forcer l'ouverture de la console et " tromper " le système de protection de la Ps2). Le système " Flip Top " permet de palier à cela : il faut démonter la Ps2 pour retirer tout le dessus de sa console, il ne reste plus qu'à utiliser le " Slide Card " et à lever le couvercle pour mettre la copie. Deux inconvénients : soit on endommage le mécanisme du lecteur de DVD, soit on ouvre la console et on perd la garantie Sony. On ne peut pas jouer avec les jeux PsX ou PsOne au moyen de cette méthode, il faut utiliser le " Breaker Pro ", le principe est le même, sauf qu'on peut uniquement jouer avec les jeux PsX et PsOne (fonctionne aussi bien sur PsX / PsOne que sur Ps2).

VOLUTION DE PS2

FAQ Voici les réponses aux questions les plus posées :

Peut-on mettre une copie de jeu dans le lecteur de la Ps2 afin de le copier sur le disque dur ?
Impossible si vous n'avez pas de puce installée dans votre Ps2, car la console ne saura pas lire le CD ou le DVD.

Peut-on relier la Ps2 sur le réseau pour envoyer directement les jeux de l'ordinateur vers la console ?
Non, il faut passer par le HDloader.

Un fois le HDloader installé, a-t-on besoin du CD ?
Oui, il faut le mettre pour pouvoir accéder au menu, donc au disque dur et aux jeux qui s'y trouvent.

Peut-on mettre n'importe quel type de disque dur ?
Pour une compatibilité à 100 %, il faut le disque dur officiel de Sony, mais il est limité à 40Go. Pour une taille supérieure, la marque conseillée est Maxtor, mais sans garantie à 100 %, pour vérifier la compatibilité http://ps2drives.x-pec.com .

Peut-on faire une copie de sauvegarde d'un jeux Playstation ?
Non, le HDloader ne fonctionne qu'avec les jeux Playstation2.
Le HDloader est-il compatible avec tous les jeux Ps2 ?
Non, certains jeux ne sont pas compatibles (heureusement ils sont rares ; voir " jeux incompatibles avec HDloader ").

Le HDloader est-il compatible avec toutes les versions de Ps2 ?
Non, mais seuls les trois premiers modèles de Ps2 japonaises ne sont pas compatibles.

Quelle est la taille maximum pour le disque dur ?
Il n'y a pas de taille maximum, mais la Ps2 n'utilisera que 137Go.

Est-on obligé d'être connecté à Internet pour utiliser le HDloader ?
Non, l'adaptateur modem est là simplement pour pouvoir connecter le disque dur.

Combien de jeux peut-on mettre sur le disque dur ?
Cela dépend, tous les jeux n'ont pas la même taille. Par exemple, si vous avez un disque de 120Go, avec une moyenne de 2Go par jeux, vous pouvez mettre 60 jeux sur le disque (c'est une moyenne, certains jeux font 4Go et plus, et d'autres moins de 2Go).

Peut-on utiliser un disque dur externe en USB avec le HDloader ?
Non, le transfert n'est pas assez rapide.
Doit-on formater le disque dur avant de le mettre dans la Ps2 ?
Non, le formatage pour la Ps2 est un formatage propriétaire (APA). Le formatage sera fait directement dans la Ps2 à l'aide du HDloader qui, le cas échéant, posera automatiquement la question.

Peut-on utiliser l'Action Replay ou autre avec le HDloader ?
Non, pour l'instant c'est incompatible.

Peut-on utiliser le HDloader pour sauvegarder ses parties sur le disque dur ?
Non.

Peut-on continuer d'utiliser la carte mémoire avec le HDloader ?
Oui.

Peut-on jouer aux jeux " On line " avec le HDloader ?
Vous pouvez jouer à tous les jeux qui n'utilisent pas le " DANS Online ".

A-t-on besoin d'une Ps2 modifiée (avec puce) pour utiliser le HDloader ?
Non, le HDloader a été conçu pour booter sur les Playstation2 d'origine.

Peut-on faire une copie du HDloader ?
Non car la Ps2 vérifie le CD/DVD ; s'il n'est pas conforme, il ne pourra pas être lu dans la console.

CONCLUSION

Points faibles du HDloader : limite de taille du disque dur, lecture de jeux PsX et PsOne impossible, introuvable dans les boutiques en France.
Points forts : très simple d'installation, ne nécessite pas l'ouverture de la console, donc on ne perd pas la garantie Sony, pas besoin de mettre une puce pour jouer avec des copies de sauvegarde, interface et notice simples à utiliser et en français, installation rapide (quelques minutes simplement).
Le HDloader permet l'utilisation d'un disque dur.
Son prix était très abordable (moins de 30 euros).

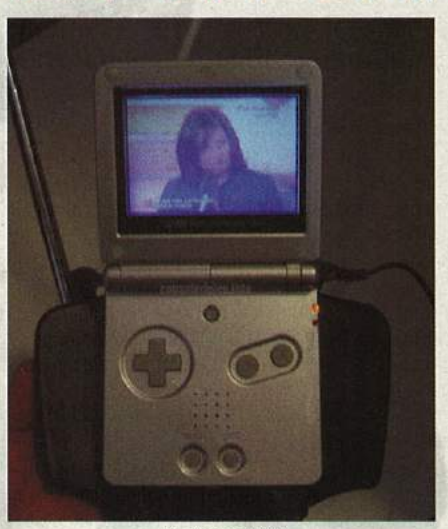
Le HDadvance est sorti pour remplacer le Hdloader. Il se présente avec deux médias :
- CD pour sauvegarder les jeux version CD,
- DVD pour sauvegarder les jeux DVD.

Pour l'instant, il n'est pas en vente dans les boutiques en France, et ne le sera peut-être jamais, donc, à suivre...

By Xavier
Webmaster de www.xavboxps2.com
(site consacré au hacking de la Ps2, PsX et PsOne)

LES EXTRAS
DE LA GAME BOY ADVANCE SP

La GBA SP sera prochainement remplacée par la Nintendo DS, pourtant cette console n'en demeure pas moins une fabuleuse petite console aux ressources surprenantes. Voici comment l'exploiter au maximum de ses capacités.



Le tunner TV

De nombreuses options apparaissent pour la GBA SP, certaines directement issues des laboratoires de Nintendo :
- Haut-parleur et casque,
- Poignée "grip" pour une meilleure prise en main,
- Câble pouvant relier plusieurs GBA SP ensemble (multijoueurs 4 personnes),
- Adaptateur connectable sur la Game Cube permettant de jouer aux jeux GBA SP sur la télévision,
- Loupe pour faciliter la vision ,
- etc.

Mais ce sont les applications "non officielles", car n'étant pas fabriquées par Nintendo et disponibles sur Internet, qui évidemment nous intéressent le plus !

Voici quelques exemples de ce que l'on peut actuellement trouver sur les boutiques du Net :
- Cartouches de sauvegarde (Flash2Advance et autres marques),
- Module Appareil photo,
- Adaptateur pour visionner des vidéos et écouter des MP3,
- Adaptateur pour visionner n'importe quelle source audio/vidéo (lecteur de DVD, magnétoscope, Nintendo Game Cube ou tout autre console),
- Skins (pour modifier l'apparence de la GBA SP),
- Tuner TV pour voir la télévision sur sa GBA SP,
- GPS pour se diriger partout,
- etc.

CARACTÉRISTIQUES DE LA GBA SP

- **écran 2.9" TFT - 32000 couleurs rétro-éclairé,**
- **82mm x 24.3mm x 84.6mm,**
- **143 grammes,**
- **son stéréo,**
- **batterie lithium ion rechargeable en 3heures,**
- **autonomie de10 heures avec lumière et de 18 heures sans,**
- **rétro compatible avec les jeux Game Boy,**
- **processeur 32-bits,**
- **coloris gris métalisé / bleu / noir,**
- **mode multijoueurs à 4 possible,**
- **peut être connectée à la Game Cube,**
- **nombreux accessoires...**

SKIN POUR GBA SP

Des autocollants prédécoupés aux dimensions de votre GBA SP vont donner un nouvel aspect à votre GBA SP. Facilement et rapidement positionnables (en quelques minutes seulement), ils donnent l'impression d'avoir une autre GBA SP. Pourquoi ne pas en changer régulièrement ?

CARTOUCHE DE SAUVEGARDE

La plus connue est Flash2Advance. Fonctionnant comme une disquette, elle permet d'enregistrer et d'effacer des ROMs. On la trouve sous différentes tailles : 128Mb / 256Mb / 512Mb et 1Gb. Vous l'aurez compris, plus la capacité est élevée et plus vous stockerez de données dessus. Pour se donner une petite idée, avec une cartouche de 512Mb (attention, ce ne sont pas 512 megaoctets, mais 512 megabits - il faut diviser par 8 pour avoir la taille en Mo) on peut mettre 1 à 16 jeux selon la taille du jeu. Comment ça marche ? La GBA SP est directement reliée au PC afin de pouvoir y mettre des ROMs, des vidéos et autres applications développées en ce sens.

Dans un premier temps, le système fonctionnait à l'aide du port parallèle, à présent la connectique se fait via le port USB, offrant ainsi un meilleur débit. La cartouche fonctionne comme une disquette : elle peut être effacée à volonté ! Il existe différentes versions de soft pour envoyer des données dans la GBA SP (voir photo), à vous de déterminer celui qui vous convient le mieux. On peut ainsi sauvegarder ses jeux et en mettre plusieurs sur la même cartouche. Fini les pertes de cartouches de jeux par le petit frère, tout est stocké sur une seule cartouche et les jeux originaux restent à la maison... Ce système permet également de voir des vidéos (démos disponibles sur Internet) ; le format est du .gba, il faut donc utiliser un soft pour les convertir.

Changer de peau ▲

Movie Player ▶

APPAREIL PHOTO POUR GBA SP

Il se connecte directement dans l'emplacement prévu pour les cartouches de jeux et transforme votre GBA SP en appareil photo. Le branchement se fait via le port USB du PC et à l'aide du câble et du soft fournis. Résolution des prises de vue : 640x480 pixels, capacité de 26 photos.

LE "MOVIE PLAYER"

Il permet de voir des vidéos et d'écouter du MP3 sur la GBA SP. Il s'emboîte à la place d'une cartouche de jeux, cependant une carte Compact Flash est requise pour la sauvegarde des données. À l'aide du soft fourni, vous convertirez les MP3 dans un format géré par la GBA SP. Le principe est le même pour les vidéos. D'une utilisation simple, il suffit de choisir le fichier à convertir sur l'ordinateur, de sélectionner le format (MP3 ou vidéo), et la conversion se fait seule. Il ne vous reste plus qu'à stocker les données sur la carte Compact Flash puis à l'insérer dans le "movie player" : la séance vidéo ou audio (MP3) débute alors...

LE TUNER TV

Sorti depuis peu dans sa version SECAM (système pour la France), il permet enfin de regarder la télévision à partir de la GBA SP ! Caractéristiques techniques : possibilité de mettre en mémoire 99 chaînes, prise casque, antenne dépliable, connectique pour antenne extérieure, entrée audio/vidéo (branchement de lecteurs tels que DVD, magnétoscope, console de jeux), fonctionne avec 4 piles ou à l'aide de l'adaptateur fourni, mais attention, l'adaptateur d'origine fourni avec le tuner ne fonctionne pas dans les prises de courant françaises (pour l'instant seul puces-et-consoles.com offre l'adaptateur secteur fonctionnant pour la France, et sans surcoût !).

Il existe bien d'autres applications pour GBA SP, que nous testerons et dont nous vous rendrons compte, en détails, si cela vous intéresse. Alors n'hésitez pas à réagir et à nous le faire savoir sur le forum de www.piratz.fr.st.

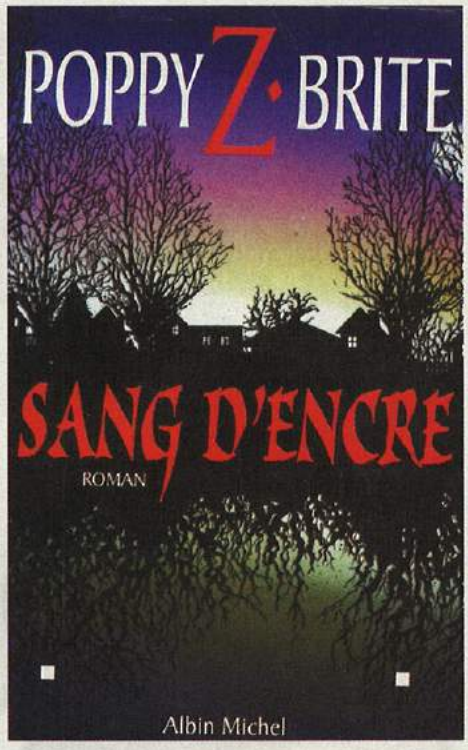
By Xavier

Webmaster de www.consoledejeux.info *(toutes les possibilités cachées des consoles passées, actuelles et à venir...)*

SANG D'ENCRE

Sang d'Encre ", de Poppy Z.Brite, est un roman qui aborde de nombreux thèmes dont, entre autres, le hacking, la démence et les maisons hantées. En d'autres termes : une bonne raison pour les geeks que vous êtes de mettre le nez dans un bouquin.

Les deux personnages principaux sont Trevor, un dessinateur de comics, et Zach, un hacker en cavale. Ce livre étant sorti en 1993, il donne un aperçu d'un hacking old school, par exemple, ne serait-ce que dans la description du matos du personnage hacker :
" Au centre du bureau, dressé au-dessus des cendriers et des paperasses tel un monolithe de plastique et de silicone, l'ordinateur. Un Amiga pourvu d'une carte I.B.M. et d'une émulation Mac qui lui permettaient de lire des disquettes provenant de plusieurs types d'ordinateurs, une chouette petite bécane. Il était équipé d'un disque dur à forte capacité, d'une imprimante correcte et - accessoire des plus importants vu l'usage qu'il en faisait - d'un modem de 2400 bauds. Cet outil bon marché, qui permettait à son ordinateur de communiquer avec quantité d'autres via le réseau téléphonique, était son gagne-pain, son cordon ombilical, la clé qui lui donnait accès à d'autres mondes et à des parties de celui-ci qu'il n'aurait jamais dû voir. "



Comme pas mal de geeks, Zach a découvert sa vocation assez jeune :
" Agé de seize ans, séparé de ses parents depuis deux ans, Zach avait quitté le système scolaire et s'était mis en quête d'une occupation plus intéressante. Il avait tout de suite jeté son dévolu sur le piratage informatique. Tout d'abord équipé d'un P.C. bon marché et d'un modem quasi-paralytique, il avait néanmoins réussi à localiser un bon nombre de serveurs clandestins, ce qui l'avait poussé à se poser des questions sur d'autres réseaux, des systèmes et des banques de données soi-disant secrets mais qui étaient en fait à sa portée, trésors tentateurs dissimulés par une barrière fragile de commandes et de mots de passe.
De l'argent et de l'information à profusion, à condition de pouvoir y accéder. Zach découvrit bientôt qu'il en était capable. Et c'était si foutrement facile... "
Seulement voilà, un beau jour il se fait balancer, et l'apprend en recevant ce message dans sa boite mail : " ILS T'ONT REPERE. ILS SAVENT QUI TU ES. ILS SAVENT OÛ TU ES. FUIS ". Il est recherché par la police. Il va donc quitter la Nouvelle-Orléans, où il vit, pour se réfugier en Caroline du Nord où il rencontrera Trevor, avec qui il va connaître des périples d'un tout autre genre comme, entre autres, une maison hantée par des sentiments de désespoir dont les murs sont restés imprégnés par la tragédie qui s'y est passée vingt ans auparavant...

L'auteur, Poppy Z.Brite, ne connaît pas grand-chose de l'informatique à la base, et s'est donc renseignée pour faire ce roman. On peut lire dans la page de ses remerciements :
" Nombre de personnes m'ont aimablement aidée dans mes recherches sur le piratage informatique. Mes plus vifs remerciements à Bruce Sterling, Dareen McKeeman, Forrest Cahoon, John Carter, et à l'underground digital dans son ensemble. Toutes les erreurs qui peuvent en subsister me sont imputables. "
Cherchez ces noms sur Google, vous ne serez pas déçus !

Le style de Poppy Z.Brite est unique et inimitable, quel que soit le sujet qu'elle aborde dans ses romans. Il est revisité d'une manière que l'on a jamais vue auparavant, que ce soit le thème du hacking et des maisons hantées dans " Sang d'Encre ", des vampires dans " Ames perdues " ou des serial killers dans " Le corps exquis ", à chaque fois son style est surprenant et ses récits rythmés, les choses racontées d'un point de vue auquel on ne se serait jamais attendu.

Elle vit à la Nouvelle-Orléans, et cette ville est souvent présente dans ses romans, son atmosphère chère à son cœur est si bien décrite que ça donne envie d'y aller faire un tour...

Quels que soient ses romans, on s'attache aux personnages, on se laisse enivrer par l'atmosphère décadente et magique de son univers.

Dark

À découvrir absolument !
" Sang d'Encre ", de Poppy Z.Brite, 1993, éditions Albin Michel
Site officiel :
http://www.poppyzbrite.com/online.html

Le conseil de Pirat'z
Vous vous dites sûrement que vous n'allez pas vous embêter à acheter un bouquin parce qu'on vous en parle dans Pirat'z. On se garderait bien, d'ailleurs, de vous en convaincre. Car en France, comme dans tous les bons pays, il y a des bibliothèques publiques !
Pour un abonnement dérisoire, et parfois une simple inscription, vous pouvez ramener à la maison presque autant de livres que vous pouvez lire. Et si ça ne vous suffit pas, sachez que vous pouvez aussi ramener des BD, des CD ou des DVD, si vous avez bien choisi votre bibliothèque. Seulement voilà, il faut les rendre au bout d'un moment.
Mais autant vous dire que c'est l'occasion de faire valoir votre droit à la copie privée.

Bonne lecture.

'Z

Du Giant au Big MS

Microsoft qui, à voir toutes les failles de sécurités de ses OS, semblait jusqu'à présent l'allié numéro un des spywares, daigne enfin se préoccuper du problème. Un mémo interne annonçait il y a très peu de temps le déploiement imminent d'une version bêta de " Atlanta ", sensé éradiquer les sale bêtes. " Tout beau, tout frais ", qu'ils disent de leur bébé, ce, quelques jours seulement après avoir racheté GIANT, une société qui fait justement des logiciels anti-spyware. Il ne s'agirait donc pas du ServicePack 2 ?

Napster in action

Napster vient d'entrer en bourse ! Coté au Nasdaq (le marché des valeurs technologiques de New York) depuis le 3 janvier, le site symbole du piratage du début des années 2000 " pèse " aujourd'hui 293 millions de dollars. Il faut dire que ce Napster-là n'a plus grand chose à voir avec celui des origines. Racheté en 2002 par la firme américaine Roxio, il ne propose plus désormais que de la musique payante. C'est pour séduire les actionnaires que Roxio a décidé de faire coter son activité sous le nom de Napster, beaucoup plus populaire que le sien.

La RIAA ne perd pas que de l'argent

L'industrie du disque vient de perdre un procès contre le fournisseur d'accès canadien Charter. Bien que la décision de la cour soit en appel, la RIAA n'a pas pu obtenir de force l'identité d'une trentaine d'utilisateurs suspectés de distribuer illégalement de la musique. Il semble en effet qu'il ne soit pas possible d'invoquer ici le DMCA, parce que les fichiers illégaux n'étaient pas stockés directement sur les ordinateurs du fournisseur. Vive le DMCA !

COURRIER DES LECTEURS

PAR KHAN

Bienfaits de la concurrence obligent (merci Google), nous voici désormais avec 250 Mo d'espace sur notre adresse piratgamez@yahoo.fr, dont seulement 3% sont utilisés, ce qui fait quand même mal au cœur. Enfin, pensez un peu aux enfants du Burundi qui n'ont rien pour stocker leurs emails, et remplissez-moi tout ça, je déteste le gaspillage ! Si possible, comme d'habitude, avec autre chose que des demandes de dépannage technique, d'adresses illégales, de sites à hacker ou de maris à cocufier (il y en avait trop, j'ai dû arrêter). Je vous souhaiterais bien une bonne année si j'en avais la place, mais tant pis, ça devra attendre l'an prochain...Khan

J'aimeré avoir une petite précision : où je pourrais me fournir le logiciel brutus ta vus quand je veut je peux bien écrire, lol) a+ merci a toi

rodney mullen

C'est assez compliqué : il faut que tu double-cliques sur l'icône " Internet Explorer " sur ton bureau, que tu tapes google.com dans la barre d'adresse, puis " brutus brute force " (sans les guillemets) dans la barre de recherche. Si tu n'y arrives pas, écris-nous et nous t'enverrons un guide complet sur CD-Rom. Je suis aussi très impressionné par tes efforts d'orthographe. Continue, tu es sur la bonne voie !

1. Je voudrais savoir si LECHATKITU possède un site web où il expose ses œuvres parce que je trouve qu'il dessine trop d'la balle ;)
2. Je compte passer de XP Pro à Linux... Est-ce que c'est une bonne chose au niveau de la compatibilité des progs et des games ????

Allan Inconnu

1. Pas de site à ma connaissance... mais il sera certainement ravi du compliment !

2. Non, ce n'est pas une bonne chose pour la compatibilité, loin de là. Pour les applications, tu devrais arriver à t'en sortir, il existe souvent soit des versions Linux, soit des logiciels émulant Windows de façon suffisamment correcte pour les faire tourner. Par contre, pour les jeux, attends-toi à avoir de sérieux soucis, car les jeux compatibles Linux sont très rares. Tu pourras trouver plus d'info sur www.linuxcompatible.org, www.linuxgames.com ou encore happypenguin.org.

Salut à toi ô tite zézette (pour une fois c'est pas ô grand maître) mdr. Pourquoi les hackers ne partent pas pour une mission du style planter tous les sites pédophiles et autres sites pornos qui ne sont pas assez protégés pour les tits n'enfants?

Angel Keeper

Merci de m'appeler ainsi, ça change agréablement ! La réponse à ta question est très simple : les sites pornos, ils les hackent bien sûr, mais pour les consulter gratis, pas pour les fermer. Pour les sites pédophiles, certains hackers vont effectivement les attaquer, mais 1) les sites de ce genre ne sont généralement pas trop publics et il n'est pas forcément évident de les trouver (non, non, je n'ai pas essayé), et 2) tous les hackers ne sont pas des robins des bois, ils ont autre chose à foutre que de protéger la veuve et l'orphelin (par exemple, hacker des sites pornos).

Salut à tous ! J'ai un problème : j'ai un pote (pas vraiment vu qu'il veut pas me le dire) qui arrive à dessiner en AOL Instant Messenger et je n'y arrive pas, est-ce que vous pouvez me dire comment on fait? SVP répondez-moi en e-mail mes parents ne veulent plus que j'achète Pirat'z.

Guizemeau

Ah, merci, ça me rappelle le bon vieux temps, quand mon frère me volait mes Lego *larme nostalgique*.

Salut l'équipe de Pirat'z. Sachant qu'on ne peut pas truquer son adresse IP sur le Net, je voudrais passer par des proxys, histoire de la cacher un petit peu ; et c'est là que les questions arrivent, notamment : quels logiciels utiliser?

GG

Par exemple, Sockschain : www.ufasoft.com/socks/. Une petite recherche sur Google t'en donnera d'autres. Un sympathique lecteur nous a d'ailleurs donné son adresse pour trouver des proxies anonymes : www.samair.ru/proxy.

Salut les pirat'z, j'ai (enfin) trouvé le lien pour la version Floppy de Linux que je cherchais après avoir lu votre HS sur Linux. Je vous envoie le lien : http://floppix.ccai.com.

Thibaut

Merci, ça pourra être utile à d'autres lecteurs qui souhaitent faire joujou avec Linux sans installer tout un gros système (Floppix tient en effet sur deux disquettes). Si d'ailleurs tu cherches d'autres distributions qui tiennent sur une ou deux disquettes, il y en a tout plein sur www.linux-links.com/Distributions/Floppy/.

Salut Khan ! Voilà, en fait j'ai créé une page identique à la page de Hotmail, sauf que lorsque l'utilisateur clique sur " connexion ", je reçois par mail son mot de passe et son adresse. Malheureusement, MSN propose une option en cas de spam ou autre pour donner l'IP du spammer et l'envoyer à l'équipe de MSN. Je voulais savoir si je risque quelque chose si un jour quelqu'un communique mon IP à MSN. Merci d'avance!

Sylvano

C'est trèèès mal ce que tu fais là. Ça s'appelle du " phishing ", et oui, tu risques gros. D'ailleurs, pour être pardonné, ta seule chance est d'aller te dénoncer toi-même sur www.anti-phishing.org.

Voilà, c'est la fin de l'année 2004 et le début de l'année 2005 alors je te souhaite une bonne année :D

Antoine

Merci, c'est très gentil de penser à moi. Ainsi qu'aux 48 autres personnes destinataires de cet email. Ça fait moins personnel tout d'un coup. Tant pis, c'est le seul message de bonne année qu'on a reçu, faut bien faire avec ce qu'on a :(

Salut Khan ça va ? Dans le monde du warez, il y a tout un jargon, et je voudrais des précisions. Pourrais-tu me dire ce que sont : dumps, dupechecks, boards, fserves, fxp ? Quand on scanne, quel est le meilleur moyen de ne pas se faire dénoncer, j'ai entendu parler des shells : tu pourrais m'en dire plus ?

KorLo

Petit lexique abrégé... **Dump** = serveur FTP sur lequel des pirates entreposent des logiciels pour les redistribuer. **Dupecheck** = essentiellement, une base de données des releases (recherches). **Board** = sans doute ici un board fxp : un forum sur lequel les gens partagent des logiciels par FXP. **Fserve** = serveur de fichier par IRC. **FXP** = protocole pour transférer des fichiers de serveur à serveur (FTP). Pour scanner, les gens utilisent généralement des proxies. Un **shell**, ici, désigne sans doute une machine hackée, utilisée pour scanner à la place de celle du hacker. Pour + d'infos : Google!

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 SECURITE INFORMATIQUE

Vulnérabilité. Actualité en français sur le hacking et la sécurité : www.vulnerabilite.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
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

ConsoleDeJeux. tout ce que vous avez toujours voulut savoir sur vos consoles de jeux, sans jamais oser le demander : www.consoledejeux.info

-Copie (gravure, modchips, ...)

Files Forums. Forums dédiés à la sauvegarde et à la gravure : www.fileforums.com
JCInfos. Un autre forum où obtenir plein d'infos sur les puces consoles : jcinfos.com
Jeux et consoles. Bon site de vente pour les puces, consoles prémodifiées et autres accessoires : www.jeux-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.org
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
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
HD loader. plus besoin de puces avec le hd loader hdloader.xavboxps2.com
ForumXboxPs2. Le forum sur toutes les puces de XBox et Ps2 : www.forum-xbox-ps2.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

-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
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