N°3 JUIN-JUILLET THE NEW ORIGINAL PIRATAGE MAGAZINE

PIRAT'Z

HACKERS & GAMERS

L 19302 9 - F: 1,50€ - RD

WAREZ : Devenez Site Operator

PIRATAGE de sites PHP • MODCHIP Xbox et PS2

Ripping • HACKER Microsoft Webserver

ANTI PUB HACKTION • NETBRUTE Scanner

CRACKEZ VRAIMENT VOS PROTECTIONS CD

EDITO

Chez Pirat'z, je ne sais pas si vous l'avez remarqué, mais nous ne sommes pas vraiment du genre à critiquer nos aimables confrères, bien qu'ils ne soient absolument pas aimables et que nous les haïssions du fond de notre coeur, ces enfoirés. Cela violerait en effet l'éthique déontologique de notre métier, érigée comme règle d'or dans notre vénérable institution. Et puis tant pis, violons-la allègrement, on n'en a rien à f***** après tout ! J'ai en effet été tenté de faire ce que je fais rarement, c'est-à-dire, non pas la vaisselle, mais aller regarder la poutre dans l'oeil du voisin au lieu de m'occuper de la paille dans le nôtre. On remarque d'abord que Pirat'z est au top de ce qui se fait en matière de nom, puisque le "Pirate" et le "Z" à la fin sont à la mode (certains allant même jusqu'à mettre un "Z" au début aussi). Bon, et que trouve-t-on à l'intérieur de tous ces jolis magazines à tête de mort ? (oui, la tête de mort est en rabais cette année, c'est pour ça qu'elle est partout). Ça dépend : il peut très bien ne rien y avoir, si vous avez eu le malheur d'acheter un mag' avec CD, et que le mag' s'avère n'être qu'un bout de carton pour accompagner les sharewares du CD. Ou bien, vous pouvez trouver des news délayées sur plusieurs pages – quand elles pourraient être synthétisées en quelques lignes – des numéros spéciaux sur la copie – tiens, ça me rappelle un hors-série Pirat'z – des articles "100% exclusifs" – sur les boards FXP par exemple, bâclant en 1 page un sujet traité en profondeur dans le Pirat'z numéro 1 – et j'en passe... Bref, il faut bien que je me rende à l'évidence : je suis vraiment le seul rédacteur en chef à ne pas lire les concurrents. Sur ce, bonne lecture de ce numéro 3 de Pirat'z, que je ne vous garantis pas exclusif, mais de qualité !

KHAN

PIRAT'Z
HACKERS & GAMERS

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

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

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

SOMMAIRE

DES ŒUFS DE PÂQUES FARCEURS !

Cela peut sembler surprenant, mais c'est vrai : les éditeurs de sites Internet sont des petits rigolos, car ils s'amusent pendant les fêtes de Pâques à cacher dans des endroits insolites des petits œufs qui déclenchent des liens un peu étranges... À l'intenaute de les trouver ! Google par exemple, qui proposait sa page d'accueil en latin sur http://www.google.com/intl/la ou le site officiel du film Matrix, sur lequel est caché un court-métrage... C'est juste pour le fun que les éditeurs font ça ; c'est en tout cas vraiment sympa !

UN ROBOT-DINO À AVOIR CHEZ SOI !

Les Japonais sont formidables ! Après avoir créé toutes sortes de bestioles virtuelles, c'est aujourd'hui Sanyo Electric qui s'y colle : l'entreprise nippone a annoncé la naissance de son dernier " bébé ", un robot qui marche sur ses quatre pattes baptisé " Banryu ". La bébête possède une magnifique corne de rhinocéros sur sa gueule et peut capter odeurs, sons et température ambiante grâce à des capteurs dissimulés sous sa carapace. Et combien coûte cette merveilleuse inutilité ? Devinez... 15 460 modiques euros ! Une affaire...

DES PIRATES AUSTRALIENS TELLEMENT RUSÉS

Ça a été chaud pour les clients de la Commonwealth Bank of Australia ! En mars dernier, ils ont reçu un e-mail semblable à ceux envoyés par leur établissement, leur demandant de " réactiver leur compte suite à des problèmes techniques ". Il fallait cliquer sur une adresse pour permettre cette réactivation, qui bien sûr, cachait une adresse IP de redirection... Les clients se trouvaient sur un site identique à celui de la banque et tapaient innocemment leurs mots de passe et identifiant, saisis au vol par les pirates ! Mais à malin, malin à demi : les victimes se sont vite rendu compte de la supercherie, car l'e-mail trompeur était truffé de fautes d'orthographes. La puce à l'oreille, ils ont contacté la banque qui a rectifié la duperie. Mais l'histoire ne s'arrête pas là : deux semaines plus tard, les pirates ultra-motivés s'attaquent de la même façon à une autre banque, la Westpac ! Puis à l'ANZ Bank... Rien ne les arrête ! Pour la police australienne, il est évident qu'ils opèrent depuis l'étranger. Un hold-up virtuel réussi en tout cas.

UN SUCCÈS QUI FAIT DES JALOUX

Le phénomène Google en irriterait-il quelques-uns ? Fort du lancement avec succès de sa formule " Google news ", le plus célèbre moteur de recherche fait des jaloux... suivez mon regard ! C'est du côté de Palo Alto, Californie, qu'on commence à s'échauffer sévère. Au siège du numéro un mondial des logiciels, Microsoft, on expérimente actuellement des formules pour lancer un moteur de recherche plus performant que Google. Cours toujours, on ne peut pas toujours être le premier partout ! Faut savoir reconnaître ses faiblesses...

RAFFARIN A SA GAME BOY

Le Premier ministre, qui ne rate pas une occasion de relancer sa cote de popularité auprès des jeunes, s'est rendu le 19 avril au Futuroscope de Poitiers pour donner le coup d'envoi de la quatrième édition de la Gamers Assembly, un des plus importants tournois de jeux vidéo en ligne. Il a assisté à une démonstration de Quake III, expliquant qu'il était " très admiratif de ce monde virtuel ", et a fini par avouer son péché mignon : la Game Boy. Il assure en posséder une et clame même avec fierté : " je suis un champion de Tétris !" Toujours le mot pour rire...

UN MINISTRE IRAKIEN QUI N'EN RATE PAS UNE

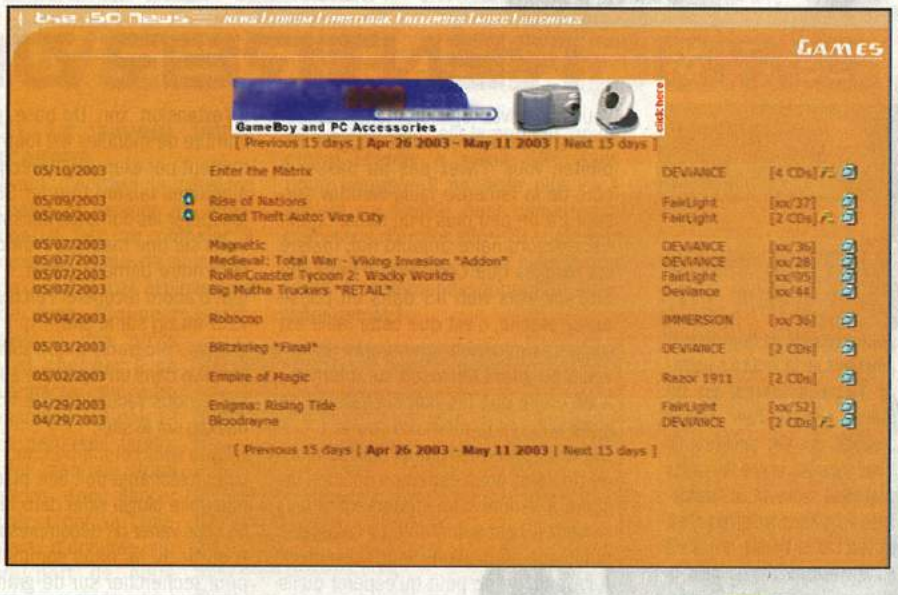
Mohammad Said al-Sahhaf, le ministre irakien de l'information, en déroute depuis la victoire américaine, est devenu une vraie star sur Internet. Un site, http://www.welovetheiraqiinformationminister.com, lui est entièrement dédié. Il a été créé par un groupe d'amis amusés et exaspérés des déclarations de pure mauvaise foi de ce ministre. Ce farceur avait en effet constamment démenti toute avancée de l'armée américaine, au mépris de l'évidence. Un optimisme à tout crin qui lui a valu un site sur ses " perles ", totalement saturé !

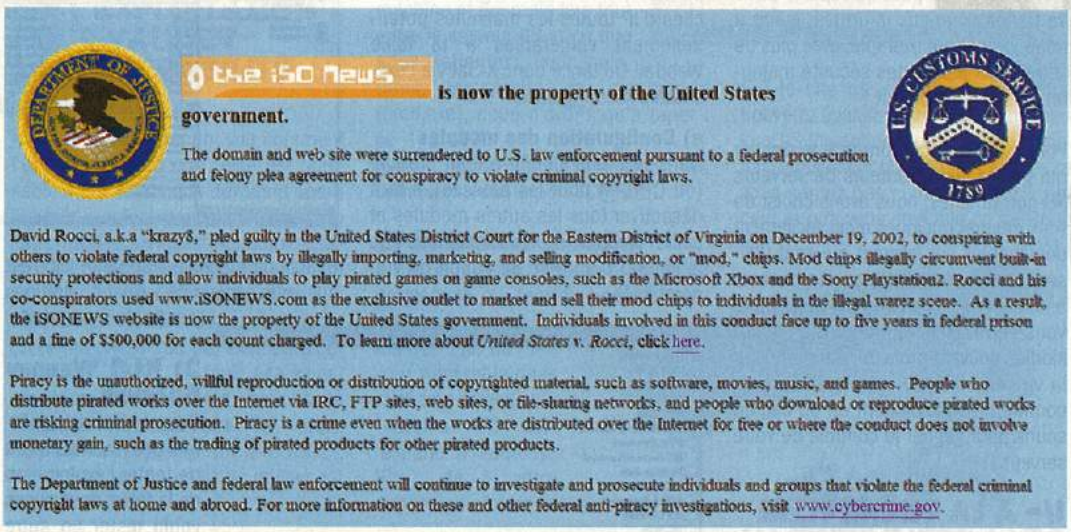
SADDAM CONVOITÉ SUR EBAY

Alors que le régime irakien s'est effondré, tout ne va pas au plus mal pour Saddam Hussein. En effet, le terrible dictateur jouissait au début du mois d'avril d'une popularité sans précédent sur le site de vente aux enchères Ebay. Tout était bon à vendre : du papier toilette avec sa photo imprimée sur chaque feuille, une adresse Internet (damnSaddam.com), des billets de dinars irakiens à l'effigie du président, des tee-shirts " la partie est finie ", et même des cibles de tir montrant le visage du tyran ! Une valeur sûre...

C'EST LA FIN D'ISONEWS.COM...

le plus célèbre site de news sur l'actualité des releases pirates a en effet été dépouillé de son nom de domaine. Son propriétaire avait en effet profité de la popularité d'Isonews pour vendre des modchips via le site. Or, avec le DMCA, les modchips sont désormais interdits aux Etats-Unis. Les autorités américaines n'ont pas laissé passer cette occasion en or de mettre fin à ce site, qui les narguait depuis longtemps en parlant en toute légalité de choses illégales. Le propriétaire du nom de domaine a ainsi accepté de le donner au gouvernement, en espérant ainsi alléger un peu sa peine. Il devra quand même passer 5 mois en prison et 5 mois coincé chez lui, en plus de devoir payer une coquette amende de près de 30000$. Ce qui n'est pas dit sur le "nouveau" site www.isonews.com ("défacé" par le gouvernement), c'est que Isonews n'est pas mort: vous pouvez le retrouver par un de ses nouveaux noms de domaine (http://www.stole-my.com/ ou http://www.izonews.com/). Un coup d'épée dans l'eau pour le gouvernement US?





RAZOR PÈTE SA COINCE

Les fichiers .NFO qui viennent avec tous les programmes piratés par les groupes de la Scène contiennent parfois des petites perles. Les groupes en profitent en effet régulièrement pour faire passer des messages personnels. Voici par exemple ce qu'on peut lire dans le NFO de Silent Hill 2, par Razor1911 (www.nforce.nl/nfos/?do=2&id=26030), en réaction à la disparition d'isonews.com: "On dirait que ce que nous avions toujours su devoir arriver est enfin arrivé. Depuis des années, Razor1911 s'est opposé à ceux qui voulaient tirer profit de la Scène. ISONEWS a toujours été l'un des pires profiteurs, et maintenant son créateur a été arrêté. Nous espérons qu'il paiera cher, et que ceux qui comptent encore profiter de la Scène changeront d'avis. De plus, Razor1911 réitère sa demande à tous les sites de news d'arrêter de poster nos nfos ou toute autre information sur notre groupe sur leur site . Nous n'apprécions pas que vous exposiez la Scène au grand public, et nous ne souhaitons certainement pas voir nos NFOs postés. Le mieux serait en fait que vous fermiez totalement, mais au moins, laissez-nous tranquille. Et pour <personne aléatoire de chez NFOrce>: ça vaut aussi pour toi!". Bon esprit Razor, par contre, comment je vais faire moi pour lire vos jolis nfos, si nforce disparaît? :-(

LE HACKING EN TEMPS DE GUERRE

La " Milice de la cyber force pour la liberté ", qui serait apparemment un groupe de hackers pro-américains, a réussi à pirater pendant plusieurs heures le site de la chaîne de télévision du Qatar Al-Jazeera. Pendant au moins deux jours fin mars, les internautes qui cliquaient pour voir la version anglaise du site étaient redirigés sur une autre page où était écrit " Que Dieu bénisse nos troupes ", alors que ceux-ci qui souhaitaient voir la version arabe tombaient, eux, sur un site... pornographique ! A la guerre, comme à la guerre !

LA LUTTE CONTRE LE P2P EST VAINE

Cela fait plusieurs années que les majors de la musique ainsi que d'autres acteurs mettent en œuvre toutes les mesures possibles et imaginables pour lutter contre les téléchargements de musique en peer-to-peer. Or, une étude menée par BigChampagne (www.bigchampagne.com), société américaine spécialisée dans l'analyse des divertissements en ligne montre que plus de 100 millions de personnes à travers le monde utilisent des logiciels d'échanges de fichiers. Et seules 9% d'entre elles ont conscience d'enfreindre la loi sur le copyright...

LES BONS POISSONS DU 1ER AVRIL

A chaque année, sa cuvée de bonnes blagues et autres poissonneries du 1er avril. Souvent lourdes, les blagues qu'on invente soi-même parviennent rarement à dérider les collègues de bureaux et amis. C'est pour cette raison que cette année, nombreux sites se chargeaient d'envoyer pour vous des blagues par email à vos amis, comme à vos ennemis. Au choix : les fausses lettres d'amour, le faux mail des impôts vous informant d'un retard ou d'une amende, la fausse lettre de la police annonçant que votre ordinateur est surveillé pour téléchargement excessif de MP3, le zoo qui vous contacte pour que vous soyez sa nouvelle attraction, ou encore la DRH qui vous annonce que vous avez pris par erreur trop de RTT et qu'il faut les rembourser... Pour les plus farceurs, d'autres fantaisies existent: les petits programmes qui déréglent les fonctions de la souris, ou font apparaître deux yeux sur l'écran de l'ordinateur, ou encore produisent un son de vitres brisées. Bref, que du bonheur ! Vivement le 1er avril 2004 pour qu'on se marre encore !

LA TRIVIALITE INSOLENTE

RENTRER DANS LES S

DO IT !

'Z

DITES-MOI QU'IL AVAIT BU!

Un responsable du Département Américain de la Justice a soutenu devant le Congrès que les réseaux Peer-to-Peer étaient contrôlés par des syndicats du crime organisé, et que les profits engendrés servaient au financement de groupes terroristes. C'est en tout cas sa théorie, même s'il n'avait aucune preuve pour la prouver. "Les barrières d'entrée sont très faibles" (c'est-à-dire qu'il est très facile d'entrer sur le marché du P2P), "et les profits énormes", a-t-il dit. De plus, d'après lui, les groupes pirates seraient des groupes criminels organisés (même s'ils ne tirent pas de profit de leurs actions), qu'il faut à tout prix anéantir. Au fait, s'il lisait Pirat'z, ce brave homme saurait que le lien entre les groupes pirates et les réseaux P2P est extrêmement ténu: en effet, les groupes ont plutôt tendance à mépriser de tels réseaux, qui attirent trop l'attention du grand public sur leurs activités. Ils préfèrent agir dans l'ombre et oeuvrer au sein d'une communauté restreinte – la Scène – plutôt que d'amasser des millions de$$$ pour financer les terroristes.

RIAA CHERCHE HEBERGEUR

La RIAA est assez malheureuse avec ses hébergeurs, étant systématiquement victime de hackers malveillants. En mars, son site web est notamment resté inaccessible plusieurs jours d'affilée. Quelqu'un a finalement découvert que l'adresse IP sous laquelle était enregistré le nom de domaine était une adresse de réseau local! Pas étonnant que le site ne fonctionne pas... Quelques jours après, la RIAA décidait de se passer des services de cet hébergeur, qui de plus était une toute petite compagnie dirigée par un militaire vétéran. Oui, c'est louche.

Vous qui suivez régulièrement l'actualité des failles et des outils pour les exploiter, vous n'avez pas pu passer à côté de la fameuse faille Webdav sortie il y a un peu plus d'un mois. Ce qui est extraordinaire aujourd'hui, malgré les ravages que Code Red a fait subir aux serveurs web IIS dans un passé assez proche, c'est que cette faille est toujours exploitable sur nombre de serveurs du géant Microsoft sur Internet. A en croire que les administrateurs de sites web ont la mémoire courte !
Cet article devrait leur donner la chair de poule et nous espérons qu'il les incitera à vérifier immédiatement si leur serveur IIS est vulnérable (à l'aide des outils que nous allons vous présenter). A l'avenir, on ne peut qu'espérer qu'ils se tiendront mieux informés, grâce à notre journal par exemple, avec plus de sérieux sur les alertes sécurité majeures qui les concernent !

Pour bien faire comprendre le danger qui guette les utilisateurs de serveurs IIS non patchés, nous avons choisi de vous montrer quelques outils facilement dénichables sur Internet qui sont utilisés quotidiennement par des hackers à la recherche d'un serveur vulnérable. Vous verrez ainsi comment les script kiddies peuvent procéder pour détecter la vulnérabilité de votre serveur puis comment ils l'exploitent en un clic de souris pour gagner le contrôle de votre serveur.

II- A LA RECHERCHE DE LA PERLE WEBDAV

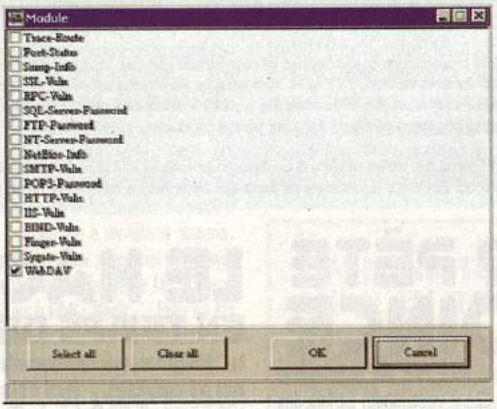
Même si il arrive que l'objectif d'un hacker soit de pirater un site particulier, la majorité de la population sur Internet cherche à exploiter une faille donnée sur des serveurs choisis aléatoirement. Les scans de port que vous récoltez quotidiennement dans votre firewall vous montrent que les ports les plus recherchés sont les ports netbios (partage de fichiers windows), le port 80 (serveur web) ou les ports attribués à des proxy (pour être anonyme sur Internet). Pour faire cela, il existe de nombreux outils qui vont scanner au hasard ou sur des plages d'IP larges les ports en question. En voici deux qui vont chercher à vérifier la vulnérabilité webdav sur les serveurs web trouvés sur un range d'adresse IP.

1) X-Scan

X-Scan est un outil assez sympathique car il s'agit d'un scanner générique. Il fonctionne avec des modules qui peuvent être ajoutés sous forme de fichiers à l'extension .xpn. De base, un certain nombre de modules est fourni, qui permettent par exemple de rechercher les machines faisant tourner SNMP pour récupérer les comptes utilisateurs existants sur une machine Windows.
Pour notre démonstration, il nous faut tout d'abord récupérer l'archive X-Scan-v2.3-en.zip sur le site http://www.xfocus.org/programs.php. Il suffit d'extraire l'archive dans un répertoire au choix. Ensuite, nous récupérons le fichier webdav.xpn sur le site :
http://www.coromputer.net/files. Le fichier téléchargé doit être placé dans le répertoire plugin situé dans le répertoire où vous venez de décompresser X-Scan. A partir de là, nous sommes équipés pour rechercher sur de grandes tranches d'IP toutes les machines potentiellement vulnérables à la faille Webdav. On lance donc X-Sat via l'exécutable xscan_gui.exe.

a) Configuration des modules

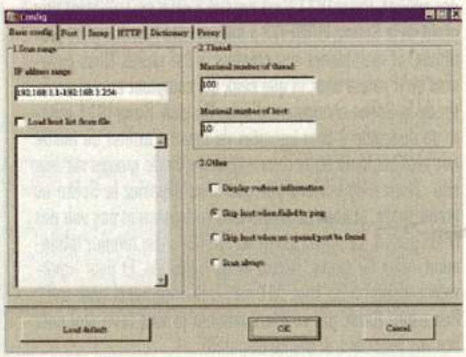
Dans le menu Config->Scan Module (ou CTRL-M pour les pressés), il faut désactiver tous les autres modules et activer Webdav (sauf si on souhaite être le champ d'analyse de l'audit de vulnérabilité).



On valide par OK et on passe à l'étape suivante....

b) La détermination de la plage d'adresses scannées

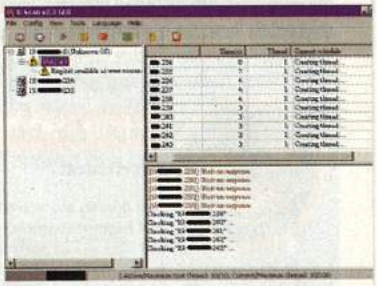
En repassant par le menu Config puis Scan parameter (CTRL-E), on peut configurer certains modules qui ne nous intéressent pas dans cet article. On aura donc juste à modifier la plage d'adresse IP scannées dans IP address range en mettant l'adresse IP de départ et la dernière adresse IP que l'on souhaite scanner.



Ici nous scannons donc tout notre réseau local à la recherche d'une machine vulnérable.
Il reste plus qu'à cliquer sur OK et on est paré pour lancer le scan. Jusqu'ici vous suivez, c'est pas trop compliqué ? ;)

c) En avant pour le scan

File->Start et vous lancez le scan de plusieurs IP simultanément. La capture d'écran suivante montre le résultat d'un scan. Vous repérez l'adresse .6 qui est vulnérable à la faille Webdav. Le scanner nous indique même où télécharger l'exploit pour rentrer sur ce serveur web IIS.

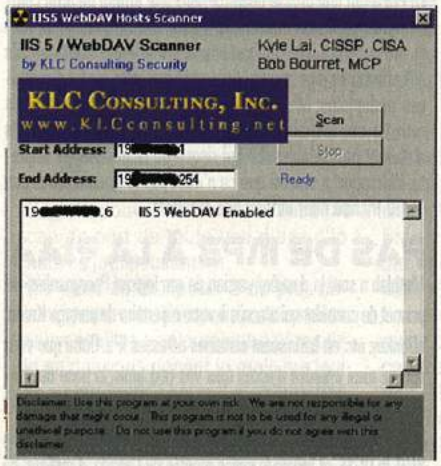


Si aucune machine n'apparaît ici, c'est que votre serveur Web n'est à priori pas vulnérable à cette faille.

2) KLC WEBDAV SCANNER

Dans le but de confirmer ces résultats avant de tenter l'exploitation de la faille, nous avons voulu tester un autre scanner de vulnérabilité Webdav : il faut récupérer le fichier IIS5_WebDAV_Scan .zip sur le site http://www.klcconsulting.net/articles/webdav/. Son interface propose de rentrer un range d'IP, et il semble plus rapide pour scanner que X-Sat, mais il oublie parfois certains serveurs (il doit vouloir aller trop vite ! ;). Testez les deux et faites votre choix.

DES EXPLOITS WEBDAV : SERVEURS WEB DE WINDOWS



III- L'EXPLOITATION POUR VALIDER LA VULNÉRABILITÉ

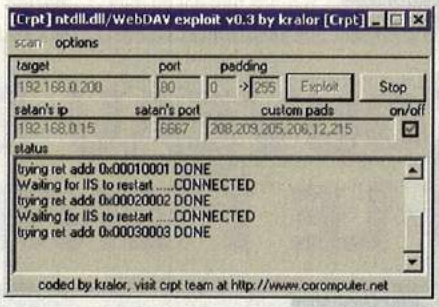
Nous allons maintenant voir comment l'exploitation de cette faille est réalisable. Pour cela, nous devons d'abord récupérer netcat pour Windows sur le site : http://www.atstake.com/research/tools/network_utilities/. Il faut ensuite le décompresser dans un répertoire étant dans le PATH (c:\winnt\system32 par exemple pour Windows 2000). Il faut également récupérer les différentes versions de l'exploit Webdav sur le site : http://www.coromputer.net/files/. La version que nous allons utiliser est la xwbf-v0.3.exe.

1) Le savoir vivre d'abord

Avant d'envoyer la cavalerie contre le serveur en question, il faut se préparer à recevoir l'invite de commande. En effet, ces exploits sont de type "Connect Back", c'est à dire qu'ils vont chercher à se connecter sur votre machine sur une IP et port qu'il faudra leur donner. Nous allons donc lancer netcat qui se chargera d'écouter sur un port de notre machine et qui redirigera tout entre le serveur IIS et ce que nous taperons. Pour cela, dans une invite de commande (cmd.exe), nous n'avons qu'à taper : nc -l -p 666
Notre netcat écoutera alors les connexions sur le port TCP 666.

2) Et ensuite le festin

Il ne nous reste plus qu'à lancer le programme qui fera du brute force pour nous.
Rentrer l'ip du serveur vulnérable dans le champ target, et la "satan's IP" correspond à l'adresse IP de votre connexion Internet.
Le "satan's port" est le port sur lequel netcat écoute, à savoir 666 dans notre exemple. Il ne reste plus qu'à cliquer sur Exploit pour démarrer le processus d'exploitation. Si vous avez de la chance, vous verrez bientôt une invite de commande apparaître dans votre netcat !



Sur le site de coromputer.net, vous trouverez également de quoi effacer les logs IIS (iis-antidote). Mais si vous souhaitez tester cet outil, c'est que vous ne vous sentez pas complètement innocent et que vous êtes allé un peu trop loin !!! :/

IZ

eDonkey bientôt interdit aux moins de 18 ans?

Le Congrès américain vient de se rendre compte que des choses pas jolies-jolies transitaient via les réseaux P2P, en matière de sexe et de pédophilie. Mon Dieu! Nous devons préserver nos chères têtes blondes! Imaginez, si un petit malin s'amusait à proposer en téléchargement des images un peu modifiées de Mickey et Minnie à la campagne... Des solutions pour lutter contre la pornographie en P2P vont donc être étudiées: que de longues heures de travail difficile pour les fonctionnaires chargés d'examiner toutes les images suspectes sur Kazaa!

LES LOIS ANTI-PIRATAGE

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

Loi N° 88-19 du 5 Janvier 1988 relative à la fraude informatique. Extraits donnés pour illustration

- **Accès ou maintien frauduleux dans un système informatique :** 2 mois à 1 an de prison, 2 000 à 50 000 francs d'amende.
- **Accès ou maintien frauduleux dans un système informatique avec dommages involontaires : modification ou suppression de données, altération du fonctionnement du système** 2 mois à 2 ans de prison, 10 000 à 100 000 francs d'amende.
- **Entrave volontaire au fonctionnement d'un système informatique :** 3 mois à 3 ans de prison, 10 000 à 100 000 francs d'amende.
- **Introduction, suppression, modification intentionnelles de données :** 3 mois à 3 ans de prison, 2 000 à 500 000 francs d'amende.
- **Suppression, modification intentionnelles du mode de traitement, des transmissions de données :** 3 mois à 3 ans de prison, 2 000 à 500 000 francs d'amende.
- **Falsification de document informatique, usage de document falsifié :** 1 an à 5 ans de prison, 20 000 à 2 000 000 francs d'amende.

EN FRANCE

PLEXTOR COMPRESSE LE TEMPS

Plextor a annoncé un nouveau graveur CDR-W capable de stocker pas moins de 980 Mo (111 min) de données sur un CD classique de 700 Mo (80 min), et 1,2 Go sur les 880 Mo (99 min). Si sa compatibilité avec les CDR(-W) existants est un bon point, il reste un problème: les CD ainsi gravés ne seront pas lisibles sur les lecteurs CD classiques. Ce produit, qui devrait être bientôt disponible, risque donc de ne pas faire le poids face aux graveurs DVD, qui sont eux de plus en plus abordables. Dommage Mr. Plextor, vous arrivez un peu en retard!

LA FORCE BRUTE CONTRE LA XBOX

Vous pouvez lire dans une autre qu'on a enfin réussi à faire tourner Linux sur une Xbox non modifiée. Mais l'autre approche envisagée pour trouver une solution à ce problème – découvrir la clef secrète qui permet de faire tourner un logiciel sur la Xbox – n'a pas pour autant été abandonnée. Le site http://operationprojectx.com/ est devenu la nouvelle page pour ce projet, qui fait appel à la puissance des ordinateurs de particuliers comme vous pour essayer de trouver la clef. Le projet est reparti, alors n'hésitez pas à y contribuer.

MAIS, MR. LE JUGE, JE LE JURE!

Le FBI a fait une grosse boulette dans une affaire de lutte contre la pédophilie sur le net. Afin d'obtenir des mandats de perquisition contre les membres d'une salle de chat suspecte, ils ont affirmé au juge que tous ses membres recevaient des images pédophiles. Mais le juge a finalement appris que seuls ceux l'ayant souhaité les recevaient, et que donc les mandats n'étaient pas valables, ce qui risque de ruiner toute l'enquête. Un rapport a montré que ce n'était pas la première fois que le FBI trichait pour obtenir des mandats.

UN NOUVEAU BUG DANS LE PENTIUM

Notre lectorat du 3ème âge doit se souvenir du fameux "bug du Pentium", à l'époque des premiers Pentium (qui atteignaient des fréquences jusqu'à 100 MHz!). Ce bug touchait le calcul en virgule flottante. Intel nous en remet une couche avec un Pentium 4 à 3 Ghz qui est atteint par un vilain bug! D'après Intel, ces anomalies ne touchent qu'"un très petit nombre de processeurs". Pas question donc d'arrêter le lancement du produit pour si peu. Au pire, si vous avez une version bugguée, vous n'aurez qu'à installer le patch 1.1.

DECSS: ON REMET ÇA

En janvier 2003, le norvégien Jon Johansen avait été acquitté dans le procès qui l'opposait à l'industrie de la musique au sujet du logiciel DeCSS. Il était accusé d'avoir écrit ce petit programme capable de cracker la protection des DVD vidéos, le premier à être popularisé sur le net. La MPAA, déçue par l'issue du premier procès, a évidemment fait appel, et c'est reparti pour un nouveau procès. J'admire l'attitude chrétienne de la MPAA, qui après s'être pris une baffe sur la joue droite, tend gentiment la joue gauche.

DES MULES PARTOUT!

eMule suscitant bien des émules, voici maintenant un projet de client... pour Java. Ce qui lui permettrait d'être compatible avec une multitude de plates-formes (pourquoi pas votre nouveau téléphone portable?). Bon bon, d'accord, il s'agit encore d'un projet, pour l'instant loin d'être terminé (v.0.01). Mais j'en ai vu tellement, des projets commencés qui n'ont jamais été terminés, que je me dis que si j'en parle dans Pirat'z, ça va peut-être motiver les p'tits gars pour mener ça au bout!
http://jmule.sourceforge.net/

FAUTE AVOUÉE À MOITIÉ PARDONNÉE

On vous rapportait dans le numéro 2 la mésaventure de cet étudiant américain de la Turlock High School, qui avait voulu prouver à l'administrateur système de son école que son réseau n'était pas aussi bien protégé qu'il le prétendait. Il avait réussi à le prouver en parvenant à accéder à une base de données confidentielle. Mal lui en a pris, puisqu'il s'est retrouvé menacé d'expulsion et de poursuites criminelles. Finalement, le conseil de l'Ecole a voté contre l'expulsion, et les poursuites seront abandonnées. C'est quand même une bonne nouvelle, car il est difficile de mettre en cause la bonne foi de cet étudiant qui est allé lui-même expliquer comment il avait pénétré dans le système! Après tout, l'école devrait le remercier pour avoir découvert une faille de sécurité, et virer son responsable sécurité à la place. Au lieu de ça, c'est l'étudiant qui devra quand même écrire une lettre d'excuses et sera interdit d'utilisation des ordinateurs du campus, pour qu'il ne fasse pas d'autres dégâts. "J'm'en fous, j'ai le password root", aurait-il déclaré.

PAS DE MP3 À LA RIAA

Methlab a sorti la dernière version de son logiciel Peerguardian qui permet de contrôler qui a accès à votre répertoire de partage Kazaa, eDonkey, etc. en bannissant certaines adresses IPs. Outre que vous pouvez ainsi interdire d'accès tous vos (ex) amis, la base de données fournie avec le programme contient également plus de 4 000 000 d'IPs appartenant soit-disant à la RIAA, la MPAA, le FBI, le KGB, la DGSE, et même la police montée du Canada. 4 millions, ça fait quand même beaucoup, ils doivent en avoir pas mal des ex-amis chez Methlab.

MOINS DE JUNK MAIL

La compagnie Microsoft a décidé de déjouer les spammers en limitant le nombre de mails qu'un usager peut effectuer à partir de Hotmail. Les spammers qui envoient des tonnes et des tonnes de mails utilisent des services comme Hotmail pour se faire de l'argent rapidement sur le dos des services de courriers électroniques gratuits. Maintenant, il sera permis aux usagers d'envoyer " un maximum de 100 " courriers électroniques à 100 adresses différentes pour une période de 24 heures. Pff, maintenant je vais devoir ouvrir 300 comptes !

SPAMMERS CHEZ AOL

Les utilisateurs de la mailling list d'AOL ont été immergés de mails " indésirables ". En effet, les pirates ont découvert une faille qui leur permettait d'usurper l'identité mail du service à la clientèle et ensuite d'envoyer des courriers électroniques à tous les usagers. Des messages sur Eminem, la guerre en Irak... ont été envoyé! Pas très méchants ces pirates. Évidemment, la compagnie est dans tous ces états à la suite de cette intrusion... et tentera de tout faire pour la sécurité de son site. Non non, ne riez pas, ils sont très sérieux.

NE LISEZ PAS CETTE NEWS, OU VOUS SEREZ FICHÉ

Simple rumeur ou réalité? Microsoft serait en train d'incorporer dans la prochaine version d'Office une méthode permettant de contrôler qui lit un certain document. Vous pourriez ainsi savoir qui a lu votre CV, ou votre dernière nouvelle érotique, voire même n'autoriser l'accès en lecture qu'à certaines personnes. Wow, ça serait vraiment génial ça, on pourrait maquetter Pirat'z sous Word, et on aurait automatiquement la liste de tous nos lecteurs! Ah non, zut, j'ai dit une grosse bêtise, si on maquette sous Word, on n'aura plus de lecteurs...

ST-MPAA FAIT SON SERMON

Toujours dans sa logique de sensibilisation au problème du piratage, la MPAA s'est fendue d'une annonce publicitaire où plusieurs personnalités de l'industrie du cinéma tentent de nous convaincre que le piratage, c'est maaaal. Georges Lucas: "Si vous continuez à télécharger des films sur Internet, je ne sortirai pas l'Episode 9, na!". Tom Cruise: "Les films sur le net c'est pourri, on ne peut pas y apprécier ma belle gueule à sa juste valeur". Hugh Grant: "Pareil que Tommy". Djamel: "Putain, chuis à Hollywood, c'est trop d'la balle!"

LES GENS S'AMUSENT PLUS AU TRAVAIL

Eh oui! Fini la torture! Une étude a démontré que les gens installent des jeux sur leur PC au boulot. Il y a donc 1/4 des personnes qui jouent au lieu de travailler, il est vrai que l'administration française a dû faire monter les statistiques. Étant donné que le " solitaire " ne les intéressent plus, ils ont besoin de plus de palpitations. Ces joueurs vont même jusqu'à télécharger des jeux sur le net ou même à apportent des copies de jeux au boulot. On comprend que certains employeurs ont peur de voir leur réseau interne exploser.

PIRATEZ EN FINESSE AVEC NETBRUTE SCANNER

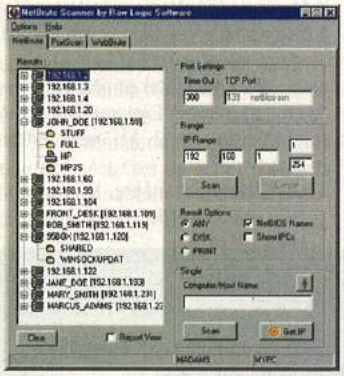
On sait bien que nos lecteurs ne sont pas des script-kiddies et que vous codez tous vos propres outils... Mais bon, juste au cas où, nous avons dégoté un tool gratuit et très (mais alors très) simple d'utilisation.

Il est composé de trois parties regroupées sous la même interface.
Imaginez pouvoir en trois clics faire un scan de port de toute une plage d'Ip choisies judicieusement.
Puis juste après passer à du plus sérieux, genre voir si quelques utilisateurs mal conseillés ;-) n'auraient pas oublié de ne pas vous donner la main sur leur PC ou sur leurs photos perso très très hot : PPPP.
Et ensuite, pour passer à des choses plus sérieuses, faire un passage par quelques sites web avec, sous les bras des dictionnaires de mots de passe bien pensés qui ouvrent les portes du bonheur des intranet les plus fous ;)))))
Voilà en quelques mots présenté l'outil, passons maintenant à la pratique;

Le module de scan de port se présente comme çà :

On va pouvoir ainsi scanner les ports Tcp issus de serveurs FTP, serveurs de Mail, serveurs Telnet, et bien sur de serveurs Web Server, ces derniers étant utiles pour le dernier module que nous verrons plus tard.
Si une classe complète c'est trop long pour vous alors le module en bas à droite permet de passer directement sur l'Ip de votre voisin de classe qui depuis une heure matte la petite blonde au lieu de filer les résultats de la prochaine intero récupérés sur le serveur web du lycée.
Bref, pas mal de possiblités s'offrent à vous par ce bel outil bien pensé.
Mais la soirée ne fait que commencer car les ports Tcp c'est bien mais les fichiers Word des CVs du prof d'informatique accessibles en écriture ça peut être pas mal, non ?
C'est là qu'arrive la seconde partie du produit, le scanner de répertoires partagés.

Un windows 2000, XP, 98 ou tout autre système ayant une ressource partagée de type partage de fichiers ou d'imprimantes Microsoft, ou toute ressource SMB compatible (i.e. Samba Servers sur une machine Unix/Linux) sera la cible rêvée.
Ensuite rebelote, il suffit de saisir un range ou une Ip et hop, le tour est joué, comme les listes ci-dessous le montrent !!!
Plus besoin de Kazaa ou autre, dans cet exemple l'Ip .59 donne un bel accès complet à son réperoire MP3'S.
Attention danger ! Protégez-vous !



Tout ça serait telllement triste si on ne pouvait pas aussi aller voir si un site web n'a pas laissé une liste de mots de passes facile à trouver pour aller grignoter quelques infos croustillantes dans ses répertoires réservés aux utilisateurs de tous poils ....
C'est là qu'intervient le dernier module (pour l'instant), qui permet alors de faire un joli tour sur tous les sites utilisant de l'authentification basique par login et mot de passe.
Même punition que précédemment, il faut cette fois non pas trouver une IP ou un range d'IP, mais un site web qui nécessite un login password pour entrer et se faire un dico ou en trouver un pas si loin... à une portée de google ;-))

Voilà, il n'y a plus qu'à montrer que vous êtes raisonnables et à vous retenir de faire quelques clics bien placés.
On peut ne pas télécharger le tool sur : http://www.rawlogic.com

QUI CONTRÔLE VRAIMENT KAZAA?

La guerre entre Kazaa et la RIAA (ainsi que plusieurs autres compagnies) est encore loin d'être terminée. Au coeur du débat, se trouve la question de savoir si Kazaa est vraiment un réseau décentralisé. En effet, comme on vous l'expliquait il y a 2 mois, Kazaa fonctionne sur le principe de supernodes: certains utilisateurs sont désignés comme étant les supernodes, et ce sont eux qui relient entre elles les différentes parties du réseau, pour communiquer les requêtes de recherche par exemple (chaque utilisateur non supernode se connectant sur une supernode). Le problème, c'est comment trouver une supernode quand on se connecte? Certains suspectent Kazaa de contrôler une supernode "racine" qui est utilisée lorsque le client Kazaa ne parvient pas à trouver d'autre supernode autour de lui. Si c'est le cas, alors Kazaa ne serait pas un réseau totalement décentralisé comme il le prétend, ce qui pourrait lui causer des ennuis en justice (c'est ce qui avait fait chuter Napster). Pour l'instant, le flou entourant Kazaa le protège encore, mais pour combien de temps?

COME GET SOME!

Avis à tous les apprentis-programmeurs de jeu, le code du célébrissime Duke Nukem 3D vient d'être mis à la disposition de tous par 3D Realms. Evidemment, on aurait préféré celui de Duke Nukem Forever, ça nous aurait permis de le finir avant eux, mais bon... A télécharger sur http://7thguard.net/files/duke3dsource.zip. Cette initiative a été saluée par la sortie de nombreuses versions modifiées, notamment pour Linux, ou en OpenGL. Pour plus d'infos, visitez donc le forum de 3D Realms qui y est consacré, sur : http://forums.3drealms.com.

DESACTIVER LE CLIC DROIT DANS UNE PAGE WEB

Nous allons voir ici toutes les méthodes actuelles concernant la désactivation du clic droit. Vous savez, quand on veut juste ouvrir un lien dans un nouvelle fenêtre, obtenir les propriétés d'un lien, voir le source ou encore enregistrer les photos sur son disque dur (que cela soit pour un fond d'écran ou autre)... et que l'on reçoit un message d'insultes accompagné d'un faux copyright genre : "Volé pa mes photo!!! le site Copyright 2003". Et bien vous aussi, vous allez maintenant pouvoir faire ch tous les visiteurs de votre site ! (dans un prochain numéro, nous apprendrons la désactivation du clic gauche, ce qui est encore plus fort !).**

1) La désactivation classique

Voici comment elle se présente :

```
<script LANGUAGE="JavaScript">
function right(e)
{
var msg = "# !?$* touche pas à mes photos >:(";
if (navigator.appName == 'Netscape' && e.which == 3)
{
  alert(msg);
}
else if (navigator.appName == 'Microsoft Internet Explorer' && event.button==2)
{
  alert(msg);
}
return true;
}
document.onmousedown = right;
</script>
```

Ici, le script tente de reconnaître le clic droit et bloque le déroulement des options en affichant l'alerte.

1ère faille du système : elle ne fonctionne que sur Netscape et Internet Explorer, donc sur un navigateur tel que Mozilla l'alerte s'affichera mais n'empêchera pas le déroulement des options !

2e faille : on peut contrer ce genre de désactivation en laissant simplement le bouton gauche de la souris appuyé pendant qu'on effectue notre clic droit...
Jusqu'ici c'est de la rigolade, voyons la suite.

2) La désactivation anti clic gauche-doit (précédente)

Voici le script qui bloque notre parade précédente :

```
<script language="JavaScript">
<!-- Begin
function right(e) {
if (navigator.appName == 'Netscape' && (e.which == 3 || e.which == 2))
  return false;
else if (navigator.appName == 'Microsoft Internet Explorer' && (event.button == 2 || event.button == 3)) {
  alert("Nanananananèère, le clic droit est désactivé !!!");
  return false;
}
return true;
}
document.onmousedown=right;
if (document.layers)
  window.captureEvents(Event.MOUSEDOWN);
window.onmousedown=right;
// End -->
</script>
```

Cette méthode ne reconnaît que les navigateurs Netscape et Internet Explorer, donc même problème que précédemment à l'exception que dans ce cas, l'ouverture avec Mozilla (par exemple) et le clic droit ne déclenche même pas l'alerte !

Bien sûr une nouvelle parade est possible, pour contre-carrer ce système, il suffit de laisser le clic droit appuyé puis d'appuyer soit sur la barre d'espace, soit Echap, soit Entrée pour refermer la fenêtre d'alerte puis de relâcher le tout : le menu s'affiche alors.

Il y a bien sûr d'autres scripts ayant les même propriétés mais codés différemment. Ils restent tout de même parables de la même manière.

3) Désactivation imparable ?

L'ultime méthode :

```
<BODY oncontextmenu="return bloque_clic()">

<SCRIPT language=JavaScript> function bloque_clic(){alert('Le clic droit est dangereux pour la santé. A consommer avec modération !');
return false;
}
</SCRIPT>
```

Cette méthode fonctionne sur tous les navigateurs ! Et n'est, à ma connaissance, pas parable. Mais si vous êtes dans un cas extrême (comme l'ancien niveau 1 de newshacker.com par exemple) vous n'avez qu'à enregistrer la page et prendre l'image souhaitée, ou, deuxième solution : désactiver le javascript !

Si c'était juste pour ouvrir un lien dans une nouvelle fenêtre, laissez tomber... et préférez le Shift ! En ce qui concerne le source, il est visible depuis Affichage->Source (dans IE).

Voilà vous savez tout (ou presque) sur la désactivation du clic droit :) Et si vous devez ne retenir que l'essentiel, ce serait que décidément, ça ne sert vraiment à rien !

Enfin, si vous connaissez d'autres trucs, que ce soit pour empêcher le clic droit ou au contraire pour contourner ces protections, n'hésitez pas à nous en faire part ! Nous publierons les meilleures astuces dans le courrier des lecteurs du numéro 1267, le concours prenant fin en décembre 2218. Un lecteur tiré au sort gagnera même le logiciel gratuit de son choix. Règlement complet du jeu disponible auprès de Me. Corbeau, sur son arbre perché.

VIVE LE PARTAGE!

Encore une petite enquête sur la mentalité des utilisateurs de P2P, qui vient de chez nos amis Américains. Parmi les adolescents, seuls 27% pensent que télécharger (ou partager) des MP3 en ligne (sans l'accord des artistes) est illégal. Chez les plus vieux (35-54 ans), ce chiffre monte faramineusement à 48%! C'est la RIAA (industrie du disque) qui doit être contente, et surtout être jalouse de sa collègue de toujours, la MPAA (industrie du film), puisque les chiffres sont différents quand on parle de films: 38% des adolescents estiment que télécharger des films est illégal, et 55% des adultes. Ouf, enfin un chiffre au-dessus de 50%! Cette enquête en ligne, effectuée par E-Poll, montre déjà que les Américains sont bien cons. Mais ce n'est pas nouveau, alors on retiendra surtout que l'industrie a encore pas mal de boulot à effectuer dans le domaine de l'éducation des mentalités. Lorsque 90% des utilisateurs de Kazaa auront conscience que ce qu'ils font est illégal, un grand pas sera franchi. Il ne restera alors "plus" qu'à les convaincre d'arrêter!

L'ENFANT TÉLÉGUIDÉ!

Le fabricant d'appareils sans fils Alcatel et Oberthur conçoivent un nouveau système de géolocalisation parental. Ainsi donc, les parents désireux connaître les moindre faits et gestes de leurs enfants le pourront dorénavant. Il s'agit de définir l'horaire de l'enfant sur son téléphone pour déterminer les points de contrôle (woohoo, des waypoints !). Le parent peut choisir le chemin, estimer le temps pour le parcourir, définir la distance maximale d'éloignement que l'enfant peut prendre,... Et pourquoi pas le téléguider tant qu'on y est ?

HACK, UPLOAD ET PHP

Nombreux sont les sites qui permettent aux visiteurs d'uploader des fichiers pour les partager avec d'autres internautes. Mais si vous utilisez un tel script d'upload sur votre site, attention ! Car, comme nous le fait remarquer un lecteur perspicace, laisser n'importe qui uploader n'importe quoi n'est pas sans danger...

"En sécurisant un site perso où les utilisateurs pouvaient uploader des images (humhum), je découvris une faille", nous écrit Cyber-Flat. Quelle faille ? Et bien, "comme beaucoup de scripts PHP pour site perso, l'upload était effectué par un script acceptant toute extension". En effet, le site ne vérifiait pas qu'il s'agissait effectivement d'images. Grave erreur, car un hacker malin peut facilement en profiter : "en me creusant un peu la tête, je décidai d'envoyer un joli script PHP tout con" :

```
<?
 $fp = fopen("index.html", "w");
 fwrite($fp, "Defaced by Cyber-Flat");
 fclose($fp);
?>
```

Ce script commence par ouvrir le fichier index.html, y laisse un petit souvenir signé, et referme le fichier. Ce n'est pas bien méchant en l'occurrence, d'autant plus que le fichier index.html en question n'est que celui du répertoire où sont stockés les fichiers uploadés. Mais imaginez, si on a accès aux fichiers principaux du site, un visiteur mal intentionné pourrait faire ce qu'il veut !

La morale de cette petite histoire : il faut bien vérifier les extensions des fichiers uploadés par les visiteurs de votre site. Nous allons voir comment sur un petit exemple, avec le script suivant, posté sur un forum de développement PHP public par un certain David, qui fait un upload non sécurisé :

```
<form enctype="multipart/form-data"
action="<?php echo
$_SERVER["PHP_SELF"]; ?>"
method="post">
<input type="hidden"
name="MAX_FILE_SIZE"
value="2048000">
File: <input name="userfile"
type="file" /><br />
<input type="submit" value="Upload"
/>
</form>

<?php
if (@is_uploaded_file($_FILES["userfile"]["tmp_name"])) {
copy($_FILES["userfile"]["tmp_name"
], "files/" .
$_FILES["userfile"]["name"]);
  echo "<p>File uploaded successfully.</p>";
}
?>
```

Pour utiliser ce script, vous devez créer un répertoire nommé "files" avec les permissions en écriture pour tout le monde, où seront stockés les fichiers uploadés par les internautes. Evidemment, ici aucune vérification n'est faite, et la méthode de Cyber-Flat fonctionne. Voici maintenant comment vous pourriez sécuriser ce script (seule la partie contenant du PHP a besoin d'être modifiée) :

```
<?php
if (@is_uploaded_file($_FILES["userfile"]["tmp_name"])) {
 $filename = $_FILES["userfile"]["name"];
 if (strlen($filename) <= 200) {
  $extension = substr($filename,
               strlen($filename)-4, 4);
   if  ($extension == ".gif" || $extension == ".jpg") {
copy($_FILES["userfile"]["tmp_name"], "files/" . $filename);
    echo "<p>File uploaded successfully.</p>";
   } else {
    echo "<p>Only GIF and JPEG
          files are accepted !</p>";
   }
 } else {
  echo "<p>Please choose a shorter
        filename.</p>";
  }
}
?>
```

On vérifie d'abord que le nom de fichier a une longueur raisonnable (moins de 200 caractères par exemple). Ce n'est pas forcément indispensable, mais ça ne peut pas faire de mal, et ça évite d'avoir trop de b***** sur votre site.

Puis on s'assure que les 4 derniers caractères (l'extension) sont bien ".gif" ou ".jpg" (si par exemple on ne souhaite accepter que des images gif ou jpeg, mais on pourrait bien sûr rallonger l'expression de test pour accepter d'autres formats). Vous pourriez aussi vouloir seulement tester que l'extension n'est pas en ".php", mais là vous prenez des risques au cas où d'autres types d'extension pourraient poser des problèmes (un exemple bête : ".php3", qui est l'extension dénotant les fichiers PHP version 3). Il vaut donc mieux lister une bonne fois pour toutes les extensions autorisées, plutôt que de rajouter au fur et à mesure qu'on se fait hacker les extensions interdites !

1Z

COMMENT ARRETER CENTROPY?

Centropy est un des groupes qui piratent des films à l'aide de caméras introduites dans les salles de cinéma, pendant la projection. Il est très difficile de lutter contre ces pirates qui disposent des dernières technologies en matière de miniaturisation (ça vous dirait de vous faire fouiller avant d'entrer au cinéma?). L'industrie du disque américaine est donc en train de développer une nouvelle arme: un brouillage de l'image, invisible à l'oeil, mais capable de perturber un enregistrement vidéo. Tant que ça ne donne pas mal au crâne...

MADONNHACK

Madonna vient de sortir son nouvel album: "American Life". Mais sur internet, on peut trouver plus de 11 fichiers musicaux différents (l'album compte 11 chansons). Pourquoi? Parce que Madonna a sorti des versions "spécial P2P", pour la grande joie des internautes, qui peuvent ainsi l'entendre dire "What the fuck do you think you're doing?" (il y a besoin de traduire?). C'est évidemment une technique de lutte contre le piratage en ligne, dont on vous parle régulièrement : le spoofing. En inondant les réseaux Peer-to-Peer de fichiers musicaux corrompus, les majors espèrent convaincre les internautes qu'il serait encore plus simple de mettre la main au portemonnaie. La nouveauté, c'est de voir la chanteuse elle-même impliquée dans l'opération. Difficile de dire si c'est une bonne chose, car avec la publicité faite autour de cette affaire, à mon avis nombreux ceux qui vont rechercher les fichiers en question par simple curiosité. Ah oui, le site web Madonna.com s'est également fait hacker peu après: "this is what the fuck I think I'm doing", ont laissé les hackers.

LES PORTS D

Votre scanner de vulnérabilité détecte qu'un port bizarre est ouvert... Etes-vous infecté par un cheval de Troie ?

PAS DE RÉPIT POUR LES INGÉNIEURS SÉCURITÉ

Un Black Hat (un hacker du côté obscur de la Force) a fait beaucoup parler de lui récemment, en publiant volontairement des vulnérabilités qui n'avaient pas encore été rendues publiques. Le hacker était parvenu à obtenir des documents provenant du CERT – un centre de recherche et de développement consacré à la sécurité informatique. Il a ainsi pu être mis au courant de certaines vulnérabilités que le CERT n'avait pas encore diffusées. En effet, le CERT partage ses informations avec un certain nombre de compagnies, afin de leur permettre de corriger les problèmes avant qu'une vulnérabilité soit rendue publique. C'est de l'une de ces compagnies qu'est venue la fuite. Le hacker, dans le seul but de créer un maximum de problèmes, a attendu le vendredi soir pour poster les vulnérabilités sur une mailing-list publique de sécurité informatique. Ainsi, les hackers avaient tout le week-end pour les mettre en oeuvre, en attendant que les responsables sécurité reviennent au boulot le lundi! Quel boulot de fou ce métier, devoir lire des mailing-lists le week-end!

LE DD-DAY

On vous annonçait dans le dernier numéro l'opération "Digital Download Day", où vous pouviez télécharger gratuitement un peu de musique sur des sites en ligne légaux. Outre que ce fut le jour le plus long, puisque l'opération a duré une semaine, qu'a-t-on pu en retirer? Tout d'abord, qu'au moins on y téléchargeait plus rapidement que sur les réseaux P2P. Par contre, les internautes ont été déçus par le peu de nouveautés disponibles. C'est normal aussi, les derniers MP3 dispos sur WinMX, ils ne sont pas encore dans le commerce!

L'UTILITÉ DES PORTS

De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (vous pouvez par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier par FTP). Chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits : un port (la combinaison adresse IP + port est alors une adresse unique au monde, elle est appelée socket). Lorsque l'ordinateur reçoit une requête sur un port, les données sont envoyées vers l'application correspondante.

Un cheval de Troie est un petit programme qui s'exécute à l'insu de l'utilisateur du système, et qui a pour but d'ouvrir un accès caché au pirate. Un trojan doit donc ouvrir un port sur la machine qu'il a infectée afin de permettre au méchant hacker de s'y connecter... C'est ce port ouvert que l'on peut détecter pour repérer ce genre de backdoor.

LA FONCTION DE MULTIPLEXAGE

Le processus qui consiste à pouvoir faire transiter sur une connexion des informations provenant de diverses applications s'appelle le multiplexage. De la même façon le fait d'arriver à mettre en parallèle (donc répartir sur les diverses applications) le flux de données s'appelle le démultiplexage.

Ces opérations sont réalisées grâce au port, c'est-à-dire un numéro associé à un type d'application, qui, combiné à une adresse IP, permet de déterminer de façon unique une application qui tourne sur une machine donnée.

ASSIGNATIONS PAR DÉFAUT

Il existe des milliers de ports (ceux-ci sont codés sur 16 bits, il y a donc 65536 possibilités), c'est pourquoi une assignation standard a été mise au point, afin d'aider à la configuration des réseaux.

VOICI CERTAINES DE CES ASSIGNATIONS PAR DÉFAUT :

Port Service ou Application
21 FTP
23 Telnet
25 SMTP
53 Domain Name Server
63 Whois
70 Gopher
79 Finger
80 HTTP
110 POP3
119 NNTP

Les ports 0 à 1023 sont les ports reconnus ou réservés (Well Known Ports). Ils sont assignés par le IANA (Internet Assigned Numbers Authority) et sont, sur beaucoup de systèmes, uniquement utilisables par les processus système ou les programmes exécutés par des utilisateurs privilégiés. Un administrateur réseau peut toutefois lier des services aux ports de son choix.
Les ports 1024 à 49151 sont appelés ports enregistrés (Registered Ports)
Les ports 49152 à 65535 sont les ports dynamiques ou privés

Ainsi, un serveur (un ordinateur que l'on contacte et qui propose des services tels que FTP, Telnet, ...) possède des numéros de port fixes auxquels l'administrateur réseau a associé des services. Ainsi, les ports d'un serveur sont généralement compris entre 0 et 1023 (fourchette de valeurs associées à des services connus).

Du côté du client, le port est choisi aléatoirement parmi ceux disponibles par le système d'exploitation. Ainsi, les ports du clients ne seront jamais compris entre 0 et 1023 car cet intervalle de valeurs représente les ports connus.

DÉTECTER UN TROJAN

Vous pouvez utiliser la version Windows de nmap, à télécharger sur http://www.insecure.org, pour scanner les ports de votre machine. Si vous repérez un port suspect, consultez la liste ci-dessous pour savoir à qui vous avez (peut-être) affaire.

Vous pourrez ensuite chercher sur google des indications plus précises sur vos suspects, pour pouvoir les enlever (à la main ou avec un antivirus). Vous pouvez aussi essayer de vous connecter au port avec l'utilitaire telnet.exe, pour vérifier s'il ne s'agit pas d'une fausse alerte (experts only). Ou bien, vous pouvez télécharger les logiciels de contrôle associés aux trojans qui vous ont infecté - toujours avec une recherche sur google - et essayer de les utiliser pour prendre le contrôle du cheval de Troie. Cela ne marchera pas, cependant, si le pirate a mis un mot de passe.

ALLEZ, ON Y VA !

port 21 - Back Construction, Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, WebEx, WinCrash
port 23 - Tiny Telnet Server (= TTS)
port 25 - Ajan, Antigen, Email Password Sender, Haebu Coceda (= Naebi), Happy 99, Kuang2, ProMail trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
port 31 - Agent 31, Hackers Paradise, Masters Paradise
port 41 - DeepThroat
port 59 - DMSetup
port 79 - Firehotcker
port 80 - Executor, RingZero
port 99 - Hidden Port
port 110 - ProMail trojan
port 113 - Kazimas
port 119 - Happy 99
port 121 - JammerKillah
port 421 - TCP Wrappers
port 456 - Hackers Paradise
port 531 - Rasmin

ES TROJANS

port 555 - Ini-Killer, NeTAdmin, Phase Zero, Stealth Spy
port 666 - Attack FTP, Back Construction, Cain & Abel, Satanz Backdoor, ServeU, Shadow Phyre
port 911 - Dark Shadow
port 999 - DeepThroat, WinSatan
port 1001 - Silencer, WebEx
port 1010 - Doly Trojan
port 1011 - Doly Trojan
port 1012 - Doly Trojan
port 1015 - Doly Trojan
port 1024 - NetSpy
port 1042 - Bla
port 1045 - Rasmin
port 1090 - Xtreme
port 1170 - Psyber Stream Server, Streaming Audio trojan, Voice
port 1234 - Ultors Trojan
port 1243 - BackDoor-G, SubSeven, SubSeven Apocalypse
port 1245 - VooDoo Doll
port 1269 - Mavericks Matrix
port 1349 (UDP) - BO DLL
port 1492 - FTP99CMP
port 1509 - Psyber Streaming Server
port 1600 - Shivka-Burka
port 1807 - SpySender
port 1981 - Shockrave
port 1999 - BackDoor
port 1999 - TransScout
port 2000 - TransScout
port 2001 - TransScout
port 2001 - Trojan Cow
port 2002 - TransScout
port 2003 - TransScout
port 2004 - TransScout
port 2005 - TransScout
port 2023 - Ripper
port 2115 - Bugs
port 2140 - Deep Throat, The Invasor
port 2155 - Illusion Mailer
port 2283 - HVL Rat5
port 2565 - Striker
port 2583 - WinCrash
port 2600 - Digital RootBeer
port 2801 - Phineas Phucker
port 2989 (UDP) - RAT
port 3024 - WinCrash
port 3128 - RingZero
port 3129 - Masters Paradise
port 3150 - Deep Throat, The Invasor
port 3459 - Eclipse 2000
port 3700 - Portal of Doom
port 3791 - Eclypse
port 3801 (UDP) - Eclypse
port 4092 - WinCrash
port 4321 - BoBo
port 4567 - File Nail
port 4590 - ICQTrojan
port 5000 - Bubbel, Back Door Setup, Sockets de Troie
port 5001 - Back Door Setup, Sockets de Troie
port 5011 - One of the Last Trojans (OOTLT)
port 5031 - NetMetro
port 5321 - Firehotcker
port 5400 - Blade Runner, Back Construction
port 5401 - Blade Runner, Back Construction
port 5402 - Blade Runner, Back Construction
port 5550 - Xtcp
port 5512 - Illusion Mailer
port 5555 - ServeMe
port 5556 - BO Facil
port 5557 - BO Facil
port 5569 - Robo-Hack
port 5742 - WinCrash
port 6400 - The Thing
port 6669 - Vampyre
port 6670 - DeepThroat
port 6771 - DeepThroat
port 6776 - BackDoor-G, SubSeven
port 6912 - Shit Heep port 6939 - Indoctrination
port 6969 - GateCrasher, Priority, IRC 3
port 6970 - GateCrasher
port 7000 - Remote Grab, Kazimas
port 7300 - NetMonitor
port 7301 - NetMonitor
port 7306 - NetMonitor
port 7307 - NetMonitor
port 7308 - NetMonitor
port 7789 - Back Door Setup, ICKiller
port 8080 - RingZero
port 9400 - InCommand
port 9872 - Portal of Doom
port 9873 - Portal of Doom
port 9874 - Portal of Doom
port 9875 - Portal of Doom
port 9876 - Cyber Attacker
port 9878 - TransScout
port 9989 - iNi-Killer
port 10067 (UDP) - Portal of Doom
port 10101 - BrainSpy
port 10167 (UDP) - Portal of Doom
port 10520 - Acid Shivers
port 10607 - Coma
port 11000 - Senna Spy
port 11223 - Progenic trojan
port 12076 - Gjamer
port 12223 - Hack´99 KeyLogger
port 12345 - GabanBus, NetBus, Pie Bill Gates, X-bill
port 12346 - GabanBus, NetBus, X-bill
port 12361 - Whack-a-mole
port 12362 - Whack-a-mole
port 12631 - WhackJob
port 13000 - Senna Spy
port 16969 - Priority
port 17300 - Kuang2 The Virus
port 20000 - Millennium
port 20001 - Millennium
port 20034 - NetBus 2 Pro
port 20203 - Logged
port 21544 - GirlFriend
port 22222 - Prosiak
port 23456 - Evil FTP, Ugly FTP, Whack Job
port 23476 - Donald Dick
port 23477 - Donald Dick
port 26274 (UDP) - Delta Source
port 29891 (UDP) - The Unexplained
port 30029 - AOL Trojan
port 30100 - NetSphere
port 30101 - NetSphere
port 30102 - NetSphere
port 30303 - Sockets de Troie
port 30999 - Kuang2
port 31336 - Bo Whack
port 31337 - Baron Night, BO client, BO2, Bo Facil
port 31337 (UDP) - BackFire, Back Orifice, DeepBO
port 31338 - NetSpy DK
port 31338 (UDP) - Back Orifice, DeepBO
port 31339 - NetSpy DK
port 31666 - BOWhack
port 31785 - Hack´a´Tack
port 31787 - Hack´a´Tack
port 31788 - Hack´a´Tack
port 31789 (UDP) - Hack´a´Tack
port 31791 (UDP) - Hack´a´Tack
port 31792 - Hack´a´Tack
port 33333 - Prosiak
port 33911 - Spirit 2001a
port 34324 - BigGluck, TN
port 40412 - The Spy
port 40421 - Agent 40421, Masters Paradise
port 40422 - Masters Paradise
port 40423 - Masters Paradise
port 40426 - Masters Paradise
port 47262 (UDP) - Delta Source
port 50505 - Sockets de Troie
port 50766 - Fore, Schwindler
port 53001 - Remote Windows Shutdown
port 54320 - Back Orifice 2000
port 54321 - School Bus
port 54321 (UDP) - Back Orifice 2000
port 60000 - Deep Throat
port 61466 - Telecommando
port 65000 - Devil

Rico (NSIA team)

Cette liste n'est bien entendu pas définitive...

BANDE DE PERVERS!

Le Journal du Net a fait sa petite enquête sur le contenu des fichiers transitant via les réseaux P2P, à partir de l'analyse de 22 millions de requêtes. Il en ressort que 85% d'entre elles concernent des films ou des MP3 (7% d'images et seulement 5% de logiciels). Ils sont également classifiés par statut: 56% sont dits "pirates" (violation du droit d'auteur), 35% pornographiques, 6% pédophiles. Voilà qui ne va pas améliorer l'image de marque du P2P. Eh, ça vous dit une section XXX dans Pirat'z? Oui? Et ben c'est pas pour demain!

LES RUSSES, CES PROS DE LA PRISE D'OTAGE

Une prise d'otage assez spéciale a eu lieu sur le net: les otages étaient des serveurs appartenant à une société de jeu en ligne (genre casino virtuel). Et les preneurs d'otages, des hackers russes. Joli tableau, hein? Ce qu'ont fait les hackers, c'est d'abord pénétrer dans le réseau interne. Puis ils ont installé un petit logiciel qui a encrypté les données sur 5 serveurs, dont l'un contenait la plupart des données sensibles de la compagnie (données clients en particulier). Ensuite, ils ont réclamé une rançon en échange de la clé permettant de décrypter les données. La rançon (dont le montant n'a pas été communiqué) a été payée, mais si 4 des serveurs ont pu être récupérés sans problème grâce à la clef des hackers, le plus important a vu ses données effacées! Elles ont finalement pu être récupérées – non sans difficultés – par une société spécialisée dans le domaine, qui n'a facturé l'opération "que" 35000$. Tiens, je crois que moi aussi, je vais aller acheter "Super Ultra Restore Data Recovery", fonder ma société, et engager des hackers russes.

BLOQUER LES PUB D'AFFICHAGE

LA LEN EN MARCHE

La LEN, c'est la Loi pour la confiance dans l'Economie Numérique dont on vous parlait dans le numéro 2. Sachez que le projet de loi a été adopté par l'Assemblée Nationale juste après le bouclage, fin février, au cours d'une séance menée à un rythme soutenu (seulement 4 heures pour les 38 articles du projet). Parmi les points cruciaux, celui de la responsabilité des hébergeurs: ceux-ci devront retirer les sites manifestement illicites sur simple plainte. Pour éviter les abus, il a été ajouté au projet de loi un paragraphe réprimant les plaintes non justifiées. Autre ajout important: si les hébergeurs ne sont pas tenus de surveiller les données qui transitent chez eux, ils "mettent en œuvre les moyens conformes à l'état de l'art pour prévenir la diffusion de données constitutives des infractions visées aux (blabla...)" – il s'agit des infractions reliées à la pédophilie, au racisme, terrorisme, crimes de guerre, etc. Voilà un sérieux problème à résoudre pour les hébergeurs, en attendant l'examen du texte par le Sénat, qui ne devrait plus tarder.

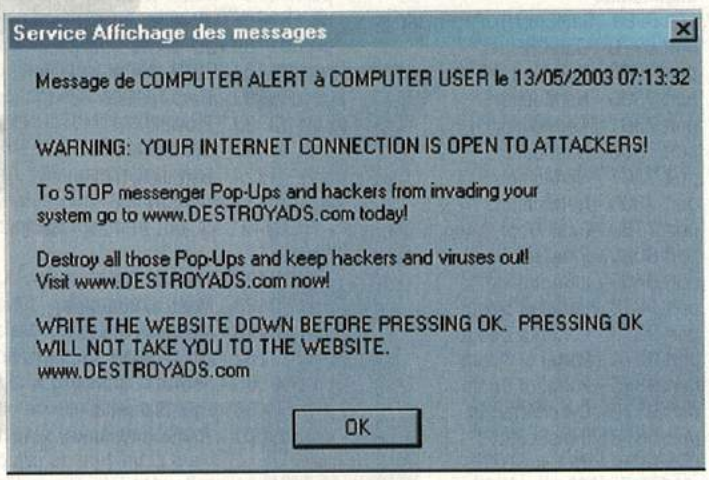
GAMECUBE: TOUJOURS RIEN

On ne désespère pas, mais le moins qu'on puisse dire, c'est qu'on ne voit toujours rien venir sur l'horizon des modchips pour la GameCube (ou le NGC, comme un sympathique lecteur nous l'a fait remarquer). Si les rumeurs vont bon train, tout ce qui semble confirmé pour l'instant, c'est que des groupes sont parvenus à ripper les jeux (en faire une image sous forme de fichier), en plaçant un périphérique intermédiaire interceptant les données entre le lecteur et la console. Bref, y a encore du boulot, alors bon courage les gars!

DO IT !

Depuis quelques mois, nombreux sont les internautes qui se plaignent de recevoir sans arrêt des messages publicitaires lorsqu'ils sont connectés. Ces messages se présentent sous la forme d'une boîte de dialogue s'affichant à l'écran, et en ce moment il n'est pas rare d'en recevoir une bonne dizaine pour une petite heure de connexion. Vu la plaie que c'est devenu, il est temps de s'en prémunir !

Tout d'abord, pour que vous reconnaissiez la bête, et pour que ceux qui ont eu la chance d'être épargnés aient une idée, voilà à quoi ça ressemble :



Si vous n'avez jamais eu affaire à ce genre de message publicitaire jusqu'à présent, soit vous utilisez un firewall; soit vous êtes encore sous Windows 9x, soit vous n'êtes pas connecté à Internet directement (voire pas du tout), soit vous êtes suffisamment malin pour être déjà passé sous Linux. Quoi qu'il en soit, si ce n'est pas le cas, voyons comment nous débarrasser de cette saleté.

1] LE FLEMMARD

Le flemmard n'a pas envie de se casser la tête, il veut un programme qui fasse tout pour lui. Chose assez énorme, de nombreux logiciels destinés à bloquer ces messages font leur pub via ce système, en vous proposant de vous protéger pour une modique somme de 20 euros ou plus !!! Evidemment, même le flemmard reste radin, et il préférera télécharger gratuitement MessageSubstract sur http://www.intermute.com/messagesubtract/.

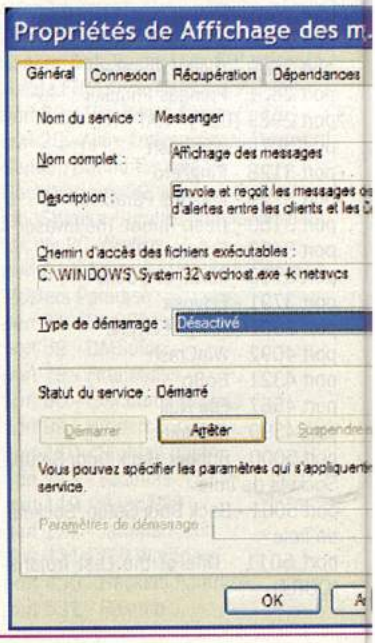
2] LE BOURRIN

Si vous voulez une solution plus radicale, vous préférerez peut-être éliminer le problème à sa source. Pour cela, il faut savoir que ces messages sont affichés par le service d'Affichage des Messages de Windows 2000/XP ("Messenger Service" pour la version américaine). Ce service, qui n'a rien à voir avec MSN Messenger ni Windows Messenger, a été conçu à l'origine pour permettre des affichages système, et la possibilité de faire passer des messages par le réseau était destinée aux administrateurs pour diffuser rapidement des informations critiques sur tout le réseau local. Malheureusement, des compagnies se sont récemment rendu compte qu'on pouvait aussi envoyer des messages par internet, ce qui est une manière simple et efficace de spammer librement. Vous aussi d'ailleurs, vous pouvez faire des blagues à vos amis en leur envoyant des messages par la commande (à taper dans démarrer / exécuter) :

net send adresse_ip Attention ! Incident système détecté: auto-destruction dans 5 secondes !

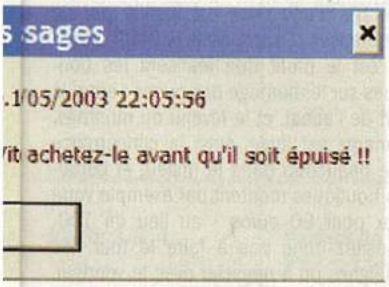
où vous pouvez mettre 127.0.0.1 comme adresse IP si vous voulez juste tester sur votre propre machine.

Ok, maintenant, que va-t-on faire ? Tuer ce service, tout simplement ! Dans le panneau de configuration, allez dans "Outils d'administration", puis "Services". Double-cliquez sur le service "Affichage des messages". Dans le type de démarrage, changez "Automatique" en "Désactivé" pour qu'il ne se relance plus, et enfin cliquez sur le bouton "Arrêter" pour lui fermer le clapet une bonne fois pour toutes, avant de cliquer sur "OK".



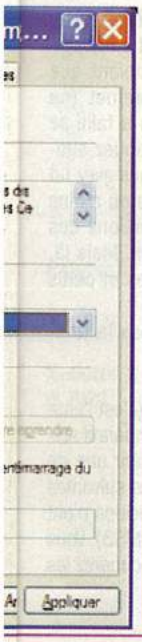
LICITES DU SERVICE DES MESSAGES

Mais attention, ce n'est pas forcément la meilleure solution, car d'autres applications peuvent utiliser ce service pour vous communiquer des messages, comme des antivirus ou certains composants du système d'exploitation. D'un autre côté, c'est l'argument qu'avance Microsoft pour tenter de nous dissuader de nous passer de ce truc inutile, donc on peut douter de sa validité, et franchement ça m'étonnerait que le service d'affichage des messages manque vraiment à quiconque. Mais bon, il existe quand même une solution plus élégante pour réduire ces pubs à néant : le firewall.



3] LE BIDOUILLEUR

La meilleure méthode consiste à bloquer l'accès au service depuis l'extérieur, afin de pouvoir toujours s'en servir sur votre propre machine. Pour cela, vous devez avoir un firewall. Le plus simple, mais certainement pas le plus sécurisé, consiste à utiliser le firewall intégré dans Windows XP. Notez qu'il vous faudra aussi le Service Pack 1, car le firewall d'origine ne bloque pas ces publicités. Le firewall s'active dans l'onglet "Avancé" des propriétés d'une connexion internet.



Il vaut quand même mieux utiliser un firewall plus perfectionné, qui vous permet de contrôler exactement ce que vous voulez faire. Et puis, après tout, le titre de cette section, c'est "le bidouilleur", et si vous vous contentez d'une case à cocher, vous ne le méritez pas ! Parmi les firewalls gratuits, je vous conseille soit :

- **ZoneAlarm :** http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp (le lien du bas)
- **Sygate Personal Firewall :** http://www.simtel.net/pub/dl/53687.html

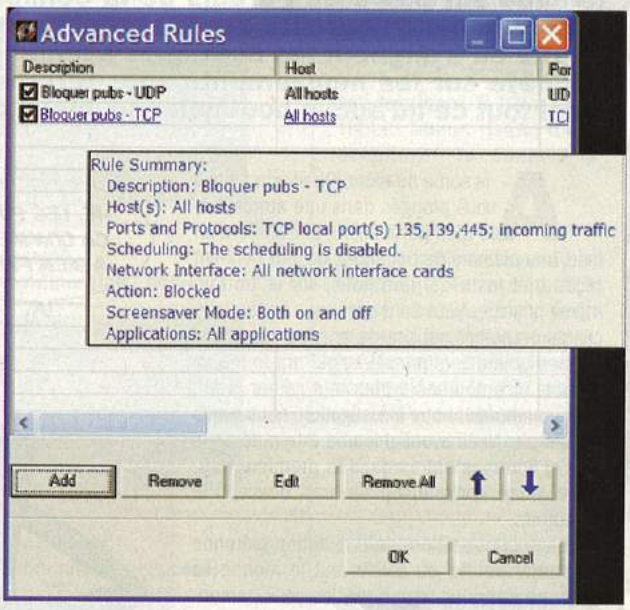
Il en existe d'autres qui vous conviendront peut-être parfaitement, mais ce sont juste ceux que j'ai eu l'occasion d'utiliser moi-même et que je peux garantir comme efficaces.

Pour isoler définitivement le service de messages, il faut bloquer les ports suivants : 135, 137 et 138 en UDP, 135, 139 et 445 en TCP. Certains de ces ports sont d'ailleurs des ports Netbios, que de toute manière il vaut mieux bloquer.

Voici la marche à suivre avec par exemple Sygate Personal Firewall :

1) Cliquer sur Tools / Advanced Rules...
2) Cliquer sur Add
3) Dans Rule Description, entrer un nom évocateur, comme "Bloquer Pubs - UDP" (on va avoir besoin de créer deux règles, l'une pour bloquer l'UDP, l'autre pour le TCP)
4) Dans l'onglet Ports and Protocols, choisir le protocole UDP, puis dans Local, mettre les ports 135,137,138, et dans "Traffic Direction, choisir Incoming

5) Cliquer sur OK
6) Cliquer encore sur Add, pour rajouter une règle qu'on appellera "Bloquer Pubs - TCP", qui cette fois-ci bloquera le protocole TCP venant sur les ports 135, 139 et 445. Après avoir cliqué sur OK, vous devez obtenir quelque chose qui ressemble à ça :



7) Cliquer sur OK, et le tour est joué, plus de pubs !
8) Si vous êtes en réseau local, vous voudrez peut-être autoriser les autres ordinateurs du réseau à se connecter sur les ports que vous avez bloqués. Pour cela, vous pouvez soit sélectionner uniquement votre connexion internet dans le champ "Apply Rule to Network Interface" de la règle, soit ajouter une nouvelle règle qui autorise (cocher "Allow this traffic" et non pas "Block this traffic" dans la règle) l'accès aux ports en question pour les adresses IP du réseau local (onglet "Hosts" de la règle). Dans ce dernier cas, pensez à mettre les règles d'autorisation tout en haut de la liste de règles, car c'est la première règle rencontrée qui prime !

Et voilà, maintenant, vous n'avez plus d'excuses pour supporter sans réagir ce spam immonde. Merci Pirat'z ! Attention quand même, si vous êtes au bureau, pensez à demander à votre administrateur avant de tout foutre en l'air sur votre bécane, de toute manière il est très probable que ce soit à lui de bloquer les pubs au niveau du firewall de l'entreprise. Si en plus vous lui faites son boulot, il ne va pas être content ! Parce que bon, quand même, ce n'était pas bien compliqué, même un administrateur réseau devrait en être capable...

LES ANGLAIS SANS P2P

Un FAI anglais, Blueyonder, a récemment proposé un changement dans le contrat d'utilisation de ses services. On y trouve notamment le paragraphe suivant: "Vous n'avez pas de droit d'utiliser ou de laisser quelqu'un utiliser nos services pour fournir des services IP de masse, y compris aux autres utilisateurs. Les services IP incluent le HTTP, les jeux, telnet, le FTP, et le Peer-to-Peer". Bref, plus de P2P, plus de serveur web ni FTP, plus de serveur de jeu... Ce sont les abonnés qui vont être contents. Ils sont fous ces Anglais!

CONSOLES : ENQUETE DES PUCES

Rendue sur place au Paradis de la console, notre équipe a récolté pour vous les dernières informations d'actualité sur le modchipping. C'est à Paris, place République, dans une grande rue où s'alignent les boutiques spécialisées dans le jeu vidéo, que nous avons mené notre enquête sur les mouvements sous-terrains relatifs aux consoles de jeux. Vous découvrirez ainsi tout ce qu'aucun boutiquier soucieux de protéger son commerce ne vous avouera jamais...

A la sortie du métro Oberkampf, nous voilà plongés dans une atmosphère bien particulière. Sur la rue d'en face, une pléthore de boutiques de jeux tiennent façade, et juste derrière nous, sur le trottoir, même principe. Nous sommes venus en tant que clients potentiels nous renseigner sur les activités des boutiquiers parisiens, qui ont formé ici un pôle incontournable pour tout gamer averti. Pour commencer notre investigation, nous avons fait simple. Nous avons pris une extrémité de la rue, et sommes entrés dans la première boutique venue, console sous le bras, direction le comptoir...

Première constatation : la population piétonne ne profite pas ici du soleil. Tout le monde se calfeutre dans les boutiques, les yeux parcourant les vitrines remplies de jeux bien rangés. Un boutiquier nous attend, l'air un peu blasé, et nous demande ce que l'on souhaite. Naïvement nous lui demandons ce qu'il peut monter comme puces pour console, et à quels prix. Le choix est vite fait. Pour la Xbox, nous pouvons installer une puce " noname " (comprendre que le fabricant n'est pas connu) avec le Bios Xecuter2, il nous en coûtera 100 euros. En revanche pour la PS2 le montage s'avère un peu plus cher : 130 euros pour une Magic 4 - voire 3, d'autres boutiques proposant une Messiah 2.

LE BUSINESS DES PUCES

Le choix de la puce au niveau des boutiques se fait selon votre version de console, mais les boutiquiers sont-ils vraiment regardants ? En effet il faut savoir qu'il y a à peu près huit versions différentes de la PlayStation 2, la Xbox n'en comptant que deux. Ainsi certaines puces sont plus faciles à monter que d'autres au niveau des branchements et des soudures, ceci en fonction de la puce et de la version de la console.

Autrement, les puces peuvent être sources de défaillances techniques sur votre console. Une puce mal montée, ou une soudure sèche, peuvent empêcher votre console de démarrer correctement (on en a fait l'expérience avec une Xbox neuve, ne rigolez pas...). Il s'agit donc de bien vous assurer auprès du vendeur que celui-ci accepte de faire les réparations gratuitement en cas de problème technique (s'il refuse, c'est un escroc, fuyez !). Il peut éventuellement y avoir d'autres sources de défaillances techniques potentielles, notamment pour la PS2. Sony a en effet eu de nombreux ratés sur les premières consoles, et essentiellement sur le lecteur. Ainsi la lecture prolongée de films DVD sur la console, peut abîmer le lecteur, ce qui, pour une console prévue en partie à cet effet, est fort regrettable... Et même pire ! Un vendeur nous a expliqué que certaines PS2 pouvaient littéralement griller si vous y lisez des DivX car le support vidéo intégré n'est pas adapté au taux de compression de certains films. Si ça sent le brûlé quand vous regardez " votre " copie de Matrix, ne vous inquiétez donc pas, c'est juste la console qui a pris la mauvaise pilule...

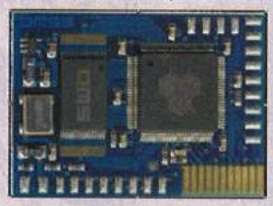
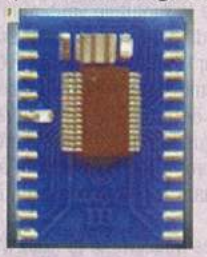
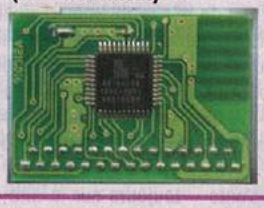
Sachez également que le prix élevé du montage d'une puce est justifié par de nombreuses raisons. Mais le motif principal est le profit que réalisent les boutiques sur le montage des puces : entre le coût de l'achat, et le revenu du montage, la marge est large. Ainsi la concurrence joue beaucoup dans le milieu, et certaines boutiques montent par exemple votre Xbox pour 80 euros - au lieu de 100. N'hésitez donc pas à faire le tour des enseignes ou à négocier avec le vendeur, si vous faites d'autres achats dans la boutique, par exemple, ou si, en bon radin, vous prétextez n'avoir que 80 euros sur vous. Actuellement certaines boutiques installent en plus sur votre Xbox, pour un prix d'environ 30 euros, l'ensemble des logiciels permettant de bidouiller la console : Evolution X, le Media Player, et plein d'autres softs plus ou moins utiles. En sachant qu'avec un peu de pratique et les bonnes adresses vous pouvez récupérer ces logiciels gratuitement - et légalement ! - sur Internet, ce choix ne s'impose qu'aux plus feignants d'entre-vous...

Il est même possible, si vous disposez déjà de la puce en pièces détachées, de la faire monter par les techniciens en boutique. C'est alors uniquement le service de montage qui est payant. A cet égard rappelons que vous pouvez acheter votre puce par correspondance sur Internet (ne demandez pas aux vendeurs quels sont leurs fournisseurs, on a failli se prendre un coup de fusil lorsqu'on a posé la question). Continuez simplement à lire et la réponse viendra toute seule. D'ailleurs, si vous avez un fer à souder chez vous, sachez que la pose d'une puce est plus ou moins facile selon votre console et sa version. Ainsi les dernières versions des PS2 sont " très dures à monter ", nous témoigne un technicien. Mais là, même avec les plans récupérés sur Internet, c'est à vos risques et périls que vous travaillez. 30
euros (le prix moyen d'un service de montage) ne valent-ils pas la tranquillité d'esprit sur la garantie de fonctionnement ?

En sachant que le montage d'une puce est - pour l'instant - légal (c'est l'usage que vous en faites qui peut ne pas l'être, ne ricanez pas), le comparatif suivant devrait informer plus allègrement tous ceux désireux d'acquérir une de ces petites bêtes. Si vous avez l'intention d'acheter une des puces suivantes pour la faire monter par quelqu'un d'autre, sachez que les techniciens n'ont peut-être pas l'habitude de monter certaines puces (comme la DMS3). Vous vous retrouveriez alors bêtement avec une puce sur les bras... Récupérez les plans de montage au passage et cela deviendra alors possible.

DANS L'UNDERGROUND

PLAYSTATION 2

NOM	CARACTÉRISTIQUES	FABRICANT	NOTES
DMS3	- Démarre automatiquement tous les supports (copies de jeux, DVD, imports, originaux, ...) - Dézonage des DVD - Démarre des applications directement depuis la carte mémoire - Mise à jour du support logiciel de la puce possible - Désactive la protection Macrovision	DMS3 (www.dms3.com) 	La puce la plus avancée sur le marché. Elle a subi de nombreux tests et est compatible sur toutes les versions de la PS2. D'après son fabricant, il n'y a quasiment aucun risque d'endommager la console à l'utiliser.
Messiah 2	- Démarre automatiquement tous les supports de jeux - Possibilité de désactiver la puce sans la dessouder	Messiah (www.messiah2.com) 	Il existe cinq versions de la Messiah 2, la version PRO étant compatible avec presque toutes les consoles (la compatibilité avec la version 4 de la PS2 européenne semblant être incertaine, et la compatibilité avec la version 8 n'est même pas assurée).
Magic 3 & 4	Permet de lire tous les jeux PSOne et PS2 sur tous supports	China Magic (www.china-magic.com) 	A l'heure où ces lignes sont écrites, le site officiel du fabricant annonce la dernière version de sa puce comme étant la Magic 3. Mais certains revendeurs prétendent fournir la Magic 4 originale. Etrange...
		XBOX	
Xtender 1.1	Permet de lire tous les supports de données (sauf les CD-R, le lecteur natif de la Xbox ne prenant pas les CD-R) et les imports	Xtender (site web mort) 	Le site du fabricant de la Xtender n'est plus en ligne. Notre avis est le suivant : si on vous la propose au montage, refusez.
Enigmah	Permet de lire tous les supports de données (sauf les CD-R)	Enigmah-X (site web fermé : www.enigmah.com)	Cette puce n'est plus en fabrication. Là encore, le site est fermé.
Xecuter 2 Lite & PRO	- Permet de lire tous les supports de données et les imports (sauf les CD-R) - Permet de lire des DVD sans la télécommande - Auto-détection d'EvolutionX (Xecuter2 LITE) - BIOS intégré sur la LITE (la Xecuter 2 PRO n'a pas de BIOS intégré, des options de programmation avancées pour bidouilleurs fous étant prévues)	Xecuter (www.xecuter2.com) 	La Xecuter 2 (PRO y compris) semble être la puce la plus développée du marché. Sur le site officiel nous pouvons lire que les CD-R ne sont pas lus sauf avec le nouveau lecteur de Samsung. En revanche certains revendeurs affirment le contraire...

Par ce comparatif on peut conclure plusieurs choses. Tout d'abord, côté PS2, c'est la DMS3 qui arrive très loin en tête, et derrière, à quasi-équivalence, la Magic 3 avec la Messiah 2. Comme vous aurez peut-être pu le constater, le site officiel du fabricant de la Magic ne fait même pas mention d'une éventuelle Magic 4. On est donc en droit de se poser des questions lorsque des revendeurs annoncent fournir la Magic 4 officielle.
Côté Xbox, c'est la Xecuter 2 qui s'impose, sans l'ombre d'un doute. Mais méfiez-vous des imitations, car ici, comme pour d'autres puces, des clones sont fabriqués et ne correspondent pas forcément à vos attentes. D'où l'intérêt de se procurer auprès de fournisseurs plutôt qu'en boutique où les commerçants achètent des puces de fabricants indéterminés, le prix étant alors plus faible.
Rajoutons également que vous ne pourrez vous fournir en puces auprès des constructeurs. Ce sont de petites sociétés qui n'ont pas les moyens de gérer la demande comme le feraient des revendeurs professionnels. Alors si acheter une puce vous tente, jetez un coup d'œil sur les sites suivants :
http://www.divineo.fr
http://www.extreme-mods.com
http://www.modchips-uk.com
http://www.hackershardware.com
(qui propose des prix attractifs)
Faites bien attention lorsque vous faites des achats sur des sites. Nous n'avons testé aucun des services d'achat des sites mentionnés ci-dessus et le mieux est encore pour vous de mener vos propres investigations (faites quelques forums pour glaner des avis par exemple). Le plus prudent reste encore de renoncer à faire vos achats auprès de revendeurs que vous connaissez mal.
Dans tous les cas, si vous êtes décidés à faire le montage vous-même, sachez que les plans de montage pour les différentes consoles sont disponibles en libre accès sur le net, comme sur le site de Divineo, revendeur international de puces pour console. Consultés par mail, les responsables de cette même entreprise ont accepté de répondre à nos questions sur quelques points spécifiques et ambigus qui nous ont intrigués. Notons au passage que cette société tient sa promesse de répondre aux e-mails en moins d'une journée, acte témoignant d'un service clientèle apparemment bien tenu.
Sur leur site nous pouvons lire que les dernières puces pour la Xbox permettent de lire tous les supports médias y compris les CD-R. Hors, d'après nos essais, très peu de CD-R passaient correctement sur la Xbox, la majorité ne passant pas du tout. Alors, quid ? " Effectivement certaines versions de Xbox ne lisent pas les CD-R. En fait le problème avec la Xbox, c'est, comme vous le savez, le lecteur. Au début, les fabricants avaient annoncé la lecture des CD-R, mais il existait de tels problèmes d'incompatibilité avec telle ou telle marque qu'ils ont retiré cette fonctionnalité. Par expérience, une fois que vous avez trouvé la marque de CD que votre console accepte, c'est bon ", nous répond-on. Notez également que la Xbox prend bien plus facilement les CD-RW que les CD-R, détail important qui vous évitera de retourner en boutique si vous rencontrez quelconque navrante difficulté.
Autre point trouble, c'est l'existence en vente - toujours sur le site de Divineo - d'une puce Magic 4, alors que le fabricant officiel ne recense que des Magic 3 dans son cursus de fabrication. Qu'en est-il réellement ? " En toute honnêteté, la Magic 4 est en fait un clone de la Magic 3. Quelques bugs ont été corrigés. Et, comme vous vous en doutez, ce n'est ni nous qui donnons le nom aux puces, ni nous qui les clonons " nous répondent encore les responsables de Divineo. A noter que cette affirmation va en contradiction avec le message sur leur site, qui, concernant les Magic 4, est assez explicite : " Attention, ceci n'est pas un clone de la Magic 4 comme il en circule beaucoup, mais la Magic 4 originale ! ". Une erreur du webmaster, ou un argument commercial un peu trop vite avancé ? C'est cependant un détail qui ne doit pas remettre en cause la bonne volonté du revendeur.
Et quant au fabricant de cette fameuse Magic 4, il est inconnu, et ce en raison du trouble réseau d'intermédiaires qui part d'Asie jusqu'aux points de vente européens officiels : une sorte de labyrinthe commercial qui laisse à penser que vous aurez bien du mal à envoyer des réclamations sur votre puce et ses fonctionnalités.

ET ÇA MARCHE LE BUSINESS À PARIS ?

Nous avons questionné quelques vendeurs en boutique pour avoir leurs impressions concernant leurs activités sur le modchipping. Après avoir essuyé quelques refus de réponse et des regards meurtriers, nous avons eu la chance de tomber sur des personnes sympathiques qui nous ont confié que c'était un marché soumis à un paradoxe.

Tout d'abord, et là les voix s'élèvent unanimement sur ce point, depuis que les puces fleurissent sur le marché, ce sont les ventes de jeux vidéo qui prennent une grosse claque en retour. Alors il est clair que l'hypocrisie du " je veux mettre une puce pour lire mes jeux imports et mes copies de sauvegarde " ne tient pas dans 95% des cas. Les vendeurs savent très bien pourquoi ils montent des puces et ce que l'utilisateur va en faire. Cela n'empêche pas une console comme le GameCube de se vendre, mais certes moins qu'une Xbox. Monter des puces devient alors une activité perverse : le profit gagné par le montage est perdu dans ce que les jeux ne sont pas vendus.

" Si nous ne le faisons pas, c'est le concurrent qui le fera... " explique un vendeur à la mine dépitée. L'obligation marketing que subissent les boutiques est bien réelle : c'est un jeu concurrentiel qui s'impose aux boutiques, et que, in facto, elles s'imposent à elles-mêmes. Un vendeur nous fait même part de sa crainte : " ce trafic peut véritablement tuer le marché du jeu vidéo et celui des magasins de jeux ". Remarque à mettre sous réserve...
Malgré la tendance, quelques irréductibles joueurs nous confient ne pas vouloir mettre de puce sur leur console, en dépit du fait que les dernières puces ne présentent que très peu de risques pour les consoles. Pourquoi ?

Julien, 23 ans, nous confie que, pour lui, jouer à des jeux que l'on n'a pas achetés, grâce aux puces, n'est pas intéressant : " on perd le goût du jeu ". De son avis, " avoir un jeu c'est avant tout prendre du plaisir à y jouer ", et ce plaisir on l'a bien plus en achetant un jeu et en s'y attelant qu'en faisant valser la collection de CD gravés sur le lecteur. C'est l'aspect collectionneur qui prime alors, mais pas seulement. En effet Julien nous confie qu'en revendant ses jeux achetés pour en racheter d'autres (via un rachat par la boutique, ou un échange) il joue à moindres frais. Il n'oublie d'ailleurs pas qu'une console patchée perd beaucoup de sa valeur à la revente, sans oublier qu'elle n'est plus garantie.

Snoop R., 25 ans, est aux antipodes de cette façon de penser. Pour lui pas question d'acheter des jeux : " ça coûte trop cher... Le montage d'une puce est rentabilisé en deux jeux gravés. Et puis ça me permet de tester les dernières nouveautés sans avoir à me vider le portefeuille ". Chez Snoop R., il y a également un autre aspect qui joue : celui du bidouilleur, du technicien. " Si j'achète une Xbox c'est pour pouvoir dépasser le niveau d'origine, pour optimiser la console. Je me fous de la garantie, je sais que si elle a un problème, j'arriverai toujours à la réparer. J'en suis pas à ma première console démontée... ", nous confie-t-il.

Les consommateurs ne sont pas les seuls à profiter de ce marché à paradoxe, car, ils ne nous l'ont pas dit, mais un vendeur nous l'a soufflé : les premières personnes à profiter des " possibilités " des puces, ce sont eux, les commerçants...

The Vocoder

ET ENCORE UN !

Un modeste employé de mairie de Digne, William Bonhomme, a écopé de deux ans de prison avec sursis pour avoir vendu 4 à 5000 CD-Roms de logiciels copiés illégalement, d'une valeur totale de 12 196 euros, à plus de 200 clients. Le jeune homme, à la tête d'un réseau de cinq informaticiens, avait été repéré et dénoncé en 1999 par des internautes, peu satisfaits d'acheter des logiciels copiés. Et ce n'est pas tout pour le pauvre bonhomme : il devra également verser 40 000 euros de dommages et intérêts à 19 éditeurs de logiciels. Ça calme !

DU PORNO
PAS VRAIMENT OFFICIEL

Un site pornographique a semé quelques vagues en Pologne ; il avait maquillé son adresse en une fausse adresse gouvernementale officielle. De quoi semer la panique chez les innocents internautes ! En effet, l'adresse du site du Parlement National http://www.sejm.gov.pl est quasi similaire à celui de notre coquin (http://www.sejm.gof.pl). Surtout si l'on sait qu'en polonais, le " v " et le " f " se prononcent à l'identique. En plus, une fois consulté, le site s'installe sur votre ordinateur. Après les histoires belges, les histoires polonaises ?

LE PIRATAGE, CAUSE DE LA RÉCESSION ?

Une étude menée à la demande des plus grands éditeurs de logiciels américains et européens montre du doigt le piratage. Selon cette étude, si le taux de copie illégale de logiciels baissait de 10 points d'ici 2006, l'économie de l'Europe y gagnerait 100 milliards d'euros de croissance et créerait 200 000 nouveaux emplois. En outre, les bénéfices issus d'une telle baisse des copies bénéficieraient directement aux industries locales et non aux groupes multinationaux. C'est en tout cas une belle façon de faire culpabiliser les pirates !

AU PAKISTAN, LES SITES PORNOS SONT DIABOLIQUES

Les intégristes ont encore sévi ! Cette fois-ci, c'est au Pakistan qu'on bloque l'accès à des sites pornographiques afin de protéger les internautes de leur influence " néfaste et diabolique ", dixit un porte-parole de la société d'Etat Pakistan Telecommunication Co. Ça tombe mal pour les surfeurs pakistanais, qui sont plus de 60% à se rendre sur les sites coquins de la Toile. Environ 1800 sites ont été bloqués depuis février 2003. Résultat : les cybercafés de Karachi ont perdu 50% de leur clientèle ! Eh les gars, les proxies, vous connaissez ?

ÇA SAQUE DUR SUR LES CAMPUS AMÉRICAINS !

L'industrie de la musique a encore frappé aux Etats-Unis : sa colère s'est tournée contre 4 étudiants, accusés d'avoir diffusé des millions de chansons sur leurs campus respectifs, grâce à leurs réseaux Internet locaux. Au menu, que des gros poissons : Springsteen, U2, Eminem ou encore Madonna. Tant d'artistes qui s'estiment lésés par les échanges de fichiers qui émanaient des campus. Aujourd'hui, les accusés risquent de payer jusqu'à 150 000 $ par titre diffusé. De quoi avoir follement envie de ressortir ses vieux 33 tours…

LE HOAX
QUI N'EN FINISSAIT JAMAIS

Cela fait maintenant plusieurs années que le même hoax tourne sur Internet : le message selon lequel la maison Veuve Clicquot offrirait une caisse de six bouteilles de champagne aux internautes qui font suivre le message à dix autres personnes n'arrête pas de se propager de boîte en boîte. Le canular le plus nul et le moins vraisemblable de la Terre continue donc de sévir. À tel point que la vénérable maison Clicquot s'est fendue fin mars 2003 d'un communiqué officiel précisant qu'elle n'était pas l'auteur de cette offre. Sans blague ?

L'UNION EUROPÉENNE SUR LE PIED DE GUERRE

Afin de lutter contre les attaques potentielles de pirates, l'Union Européenne a décidé récemment d'harmoniser les lois anti-piratage courantes dans les pays européens. D'ici le 31 décembre 2003, ils devront se mettre d'accord, sous peine de sanctions. Jusqu'ici, il est vrai qu'aucun plan d'envergure n'avait été mis à l'œuvre contre le cyber crime, qui profitait des lacunes juridictionnelles ou des législations libérales pour prospérer en toute impunité. C'est en tout cas un sévère coup de vis qui s'annonce.

ÇA HACKE SÉVÈRE À MEXICO !

Incroyable mais vrai : un pirate de génie est parvenu à piller des dizaines de comptes d'une des plus grandes banques du Mexique, détournant ainsi par Internet quelques 1,5 millions de pesos (soit environ 130 000 euros) ! La banque, la Banamex-Citibank, était située dans l'Etat de Nuevo Leon, au nord du pays. Le pirate a eu la bonne idée de repérer les comptes de clients qui n'avaient pas de mouvements réguliers. Il court toujours, à la fureur des banquiers et des clients lésés. Eh, gringo, si tu nous lis, fais gaffe à tes fesses !

UN COURS À LA FAC
POUR TOUT SAVOIR SUR LE CODE

Microsoft, en association avec l'université anglaise de Leeds, développe actuellement un cours sur la sécurité informatique. Celui-ci a pour objectif de permettre aux développeurs d'identifier les failles potentielles que les pirates cherchent à exploiter. La sécurité est en effet devenue un aspect central de tout apprentissage informatique, si l'on considère le nombre de piratages quotidiens. Microsoft espère ainsi motiver d'autres universités à prendre en compte cet enjeu au plus vite en l'intégrant dans leurs programmes.

MICROSOFT DÉVOILE SON CODE

Après le code source de Windows gracieusement fourni à certains gouvernements, Microsoft a gentiment offert au monde entier un code permettant d'installer le tout nouveau Windows Server 2003. Enfin, ils ne l'ont pas vraiment fait exprès non plus, puisque la fuite proviendrait d'une compagnie cliente. Billou n'étant pas content, il a annoncé qu'il allait lui-même faire fermer tous les sites web warez proposant le code en question. Il est malin le Billou, il cherchait une bonne occasion pour visiter quelques sites XXX au boulot…

HACKER REPENTI ?

Les hackers peuvent apporter quelque chose au niveau de la sécurité informatique d'une entreprise, car ils ont une expérience du terrain bien plus grande que ceux qui se sont contentés d'une formation classique en sécurité. Mais tout le monde ne pense pas ainsi: le grand manitou sécurité chez HP a ainsi déclaré qu'embaucher un hacker était un risque inacceptable pour une compagnie (et pour son image auprès de ses actionnaires). Pauvre Kevin Mitnick, c'est pour ça qu'il a créé sa société, personne ne voulait de lui…

LA MULE AURA SA FERME

eFarm est un projet de serveur pour le réseau eDonkey, spécialement optimisé pour fonctionner avec le client eMule. Attention, j'ai bien dit projet, hein, puisqu'à l'heure où j'écris, la seule version disponible est la 0.1 Alpha, autant dire que la mule risque de brouter un peu au démarrage. Cela dit, c'est un projet intéressant, même s'il reste encore du boulot avant de s'imposer comme le meilleur serveur. Alors, si vous voulez y jeter un coup d'oeil, la ferme en construction se trouve sur http://www.efarm-project.net/.

CHERCHER MALIN SUR EDONKEY

Vous connaissez sans doute jigle.com, un moteur de recherche très populaire pour trouver des fichiers sur le réseau eDonkey (il permet une recherche plus étendue que la recherche de base dans votre client eDonkey – ou eMule). Il existe une nouvelle alternative, un moteur de recherche de recherche au look googlien: eMoogle, à voir sur www.emoogle.com. Bien qu'il soit pour l'instant dans une langue bizarre, ça reste un moteur de recherche, donc tout lecteur de Pirat'z au QI supérieur à 20 (j'espère qu'il y en a) devrait s'en sortir.

LE SOCIAL ENGINEERING, ÇA MARCHE

Une étude récente menée par les organisateurs de la conférence "Infosecurity Europe" a montré que 90% des employés interrogés étaient prêts à révéler leur mot de passe. Evidemment, la question n'était pas directe: ce sont des spécialistes du Social Engineering qui ont "cuisiné" les victimes. Le Social Engineering consiste à gagner la confiance de quelqu'un pour l'amener progressivement à dévoiler des informations confidentielles. Comment apprendre aux gens à fermer leur gueule, voilà le grand défi de la sécurité informatique d'aujourd'hui.

COMMENT CRACKER

Les protections CD sont capitales dans le monde du jeu PC, surtout depuis que n'importe qui peut télécharger tous les derniers jeux sur eDonkey. Mais comment faire face à tous ces groupes pirates entièrement dévoués à cracker les jeux dès leur sortie ? Nous allons voir quel genre de protection on peut mettre en place... et quelles sont les techniques utilisées par les crackers pour les contourner.

STARFORCE FAIT LE FIER

StarForce est une "petite" compagnie qui développe des protections logicielles. Voulant manifestement se faire un nom, elle se distingue par une grosse activité marketing visant à vanter les bienfaits de sa dernière version (protection StarForce 3.0). Le but étant de parvenir à séduire les gros éditeurs, pour l'instant fidèles aux classiques que sont SafeDisc et SecuRom. StarForce édite ainsi, depuis février, un magazine électronique mensuel dédié à l'actualité de la protection contre la copie. On y trouve en particulier un tableau montrant les dates de sortie des jeux dans le commerce, comparées aux dates auxquelles ils ont été crackés. Pour l'instant, on n'y voit que très peu de jeux protégés par StarForce. Le premier arrive dans l'édition d'avril: il a tenu 3 semaines (un record de durée) avant qu'il soit cracké, bravo! Moi, j'attends avec impatience la prochaine édition, puisque "Word War II: Frontline Command", sorti le 2 mai, a été cracké le 7... soit le lendemain de la mise en ligne sur le site de StarForce d'une news sur ce jeu protégé par leurs soins!

ÉTEIGNEZ VOS PORTABLES !

Rien à faire : le citoyen étant incapable de se discipliner lui-même, la municipalité de New York a décidé de sévir. Depuis le dimanche 13 avril, tout gêneur qui voudra utiliser son téléphone portable dans un lieu public comme les théâtres, les bibliothèques, les musées, les cinémas ou les salles de concert se verra infliger une belle amende de 50 $ (environ autant d'euros) ! De quoi convaincre rapidement les plus récalcitrants de laisser leurs portables au vestiaire... Vivement qu'une telle mesure arrive en France !

C'est bien connu, le piratage ne fait pas du bien aux chiffres de ventes des éditeurs de logiciels. Basiquement, on peut distinguer deux types de piratage :
- la copie CD : il s'agit juste de faire une copie 1:1 (cela signifie une copie exacte du CD). En effet, il est évident que si vous arrivez à dupliquer le CD pour en obtenir un autre complètement identique, il n'y a aucun moyen pour que le programme copié se rende compte qu'il ne s'agit pas de l'original. Toute l'astuce de la protection consiste donc à écrire sur le CD des informations qui ne sont pas gravables sur un graveur personnel. Malheureusement pour les éditeurs, au fur et à mesure que leur protection s'améliore, les graveurs du commerce proposent de nouvelles fonctionnalités pour parvenir à les copier. Par exemple, pour la protection SafeDisc il suffit d'avoir un graveur supportant le mode d'écriture "DAO Raw", ce qui est désormais très courant. Les logiciels de gravure sont également de plus en plus sophistiqués, et font le maximum pour essayer de permettre à leurs utilisateurs de copier sans soucis : il s'agit de CloneCD, DiscJuggler, BlindWrite, Alcohol 120 %, et j'en passe...
- le crack : s'il est trop difficile de copier le CD, on peut toujours essayer de cracker le programme, c'est-à-dire de le modifier pour l'empêcher de se rendre compte qu'on l'exécute sur un CD copié. C'est ce dont nous allons parler dans cet article, qui va donc être d'un niveau plus technique que la moyenne, soyez prévenu ;-)

UN PROTECT.EXE, ÇA SUFFIT ?

Une première méthode pour cracker un jeu est simplement de chercher sur le net un logiciel qui va le faire à notre place (comme unSafeDisc pour SafeDisc). C'est facile, c'est rapide et ça peut rapporter gros en amende pour violation de copyright. Mais le but de l'article étant aussi de voir comment fonctionne une protection, on va se retrousser les manches et mettre soi-même les mains dans le cambouis... que va-t-on donc pouvoir trouver ?
Tout d'abord, le principe de base d'une protection CD est en gros le suivant :
- empêcher le cracker de l'analyser, en refusant de s'exécuter normalement lorsqu'est détectée une activité de crack
- vérifier que le CD original est bien présent, en y analysant les zones "spéciales" (en théorie non copiables)
- décrypter les fichiers du jeu (qui ont été encryptés pour les protéger), si possible en utilisant une information non copiable présente sur le CD
- faire diverses vilaines choses pendant l'exécution du jeu.

Bref, face à une protection un minimum sophistiquée, le cracker va devoir s'armer de bons outils – et de patience. Vous avez ce qu'il faut ? Bon, pour la patience je ne peux pas vérifier, mais côté outils, vous allez avoir besoin de:
- SoftIce (http://www.compuware.com/products/driverstudio/softice/), le débuggueur ultime pour Windows. Un débuggueur permet de tracer l'exécution d'un programme pour analyser son fonctionnement. Malheureusement, SoftIce n'est pas gratuit, et aucun shareware n'arrive à son niveau... Il existe bien OllyDbg (http://home.t-online.de/home/Ollydbg/), mais il ne s'agit pas d'un débuggueur système comme SoftIce (il opère à un niveau plus élevé du système d'exploitation), et il risque fort de s'avérer insuffisant. Notez que sous Windows XP, vous aurez besoin d'une des dernières versions de SoftIce.
- FrogsIce (http://66.36.228.12/protools/files/debuggers/frogsice.zip) un logiciel fort utile pour cacher SoftIce. Comme SoftIce est très utilisé parmi les crackers, les protections vont souvent chercher s'il est actif (il y a beaucoup de méthodes différentes pour cela), et refuser de s'exécuter si c'est le cas. FrogsIce connaît de nombreuses méthodes de détection, et est capable de les prendre en défaut, et donc de rendre SoftIce (presque) invisible. Malheureusement, il ne tourne que sous Windows 98... il est donc temps de ressortir votre vieil OS du carton ! Une alternative pour NT se nomme ntAll (http://66.36.228.12/protools/files/debuggers/ntall.zip), mais n'est pas aussi perfectionnée.
- IceDump (http://ghiribizzo.virtualave.net/icedump/icedump.html), une extension officieuse de SoftIce qui sert à "dumper" la mémoire, c'est-à-dire à la copier sur le disque dur.
-ProcDump(http://www.newhua.com.cn/down/pdump32.zip), une alternative à IceDump, indépendante de SoftIce, et qui en plus possède d'autres fonctionnalités, comme l'édition de la structure de fichiers exécutables.
- HexWorkshop (http://www.hexworkshop.com/), un éditeur hexadécimal shareware. N'importe quel autre éditeur fera sans doute aussi l'affaire, mais HexWorkshop est un bon choix pour ce que nous voulons faire.

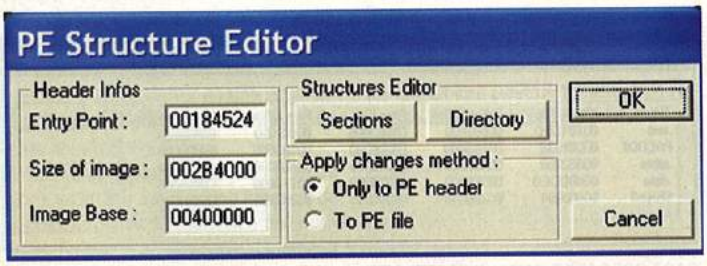
TROMPER L'ENNEMI

Il y a tellement de choses à dire sur les protections CD que nous n'allons certainement pas en faire le tour dans ce seul article, qui se veut plutôt une introduction. Si vous en voulez plus, écrivez au journal pour avoir une suite dans le prochain numéro ! Afin de passer en revue les différents points de la protection, nous allons prendre l'exemple de SafeDisc, qui est certainement – à l'heure actuelle – la protection la plus répandue. Et pour commencer, attaquons-nous plutôt à sa version 1 (maintenant, on en est à SafeDisc 2, mais mieux vaut ne pas commencer par le plus compliqué)... le nom du jeu que je vais utiliser n'est pas dévoilé pour éviter d'avoir des ennuis, appelons donc le "Toto". Vous êtes prêt ? On y va !
Je suppose que vous avez sagement installé SoftIce. Vous lancez Toto.exe... et Oh, surprise ! Il plante (blabla opération non conforme). Petit truc en passant : lorsqu'un plantage survient, SoftIce va l'intercepter (pour qu'on puisse débugguer, justement). Vous pouvez alors vous retrouver incapable de sortir de SoftIce, et, il faut taper "Faults Off" pour ne plus intercepter les erreurs, et laisser Windows les gérer tout seul. Ensuite, Ctrl-D pour sortir de SoftIce, et le tour est joué.
Bon, la première solution serait d'essayer de comprendre pourquoi ça plante en traçant le programme... Mais comme on sait que SafeDisc est vicieux, on se doute bien que c'est sa faute. Il faut donc camoufler SoftIce. On peut le faire à la main, mais le plus simple (sous Windows 98) reste d'utiliser FrogsIce. Donc, lancez FrogsIce. Faites un clic droit sur son icône dans la barre des tâches, et décochez l'option "Blue Screen of Death" - qui affiche un écran bleu lorsqu'il détecte qu'un programme cherche SoftIce. Relancez Toto... Ca marche ! Tout va bien, on peut commencer...

LES PROTECTIONS CD

Où est le programme ?

En fait, Toto.exe n'est pas vraiment le programme du jeu. Il s'agit plutôt d'un exécutable SafeDisc, qui va par exemple vérifier que vous avez bien le CD dans votre lecteur. Ensuite, il va décrypter le vrai programme, qui est codé dans le fichier Toto.icd. Ce que nous voulons, c'est nous débarrasser de Toto.exe, et ne conserver que le programme décrypté depuis Toto.icd.
Pour cela, nous allons arrêter le jeu après qu'il ait été décrypté, mais avant qu'il ait commencé à s'exécuter, en l'arrêtant exactement à son début, appelé l'OEP (Original Entry Point). Lançons ProcDump, cliquons sur "PE Editor", et sélectionnons Toto.icd. Oh magie, on apprend ainsi que l'entry point est en 184524, et que l'Image Base vaut 400000. Pour obtenir l'OEP, on additionne ces deux chiffres (qui sont en hexadécimal, attention, voire l'encadré pour ceux qui ne connaissent pas), ce qui nous donne OEP = 584524.



Maintenant, on lance Toto.exe : s'affiche un écran de titre. Si on presse Ctrl-D pour aller dans SoftIce, on voit en bas à droite "Kernel32" : on n'est pas encore dans notre programme Toto.. Ctrl-D pour sortir, on attend 1s, on refait Ctrl-D... pas encore ! On continue... finalement, on doit arriver à voir marqué "Toto" en bas à droite. Là, si on tape la commande suivante dans SoftIce :
u 584524 (désassembler à partir de l'OEP)
Si on voit quelque chose comme :
INVALID
INVALID
INVALID
....
alors dans ce cas, le fichier n'a pas encore été décrypté. On presse Ctrl-D, Ctrl-D rapidement, on appuie sur la flèche vers le haut dans SoftIce pour rappeler la dernière commande (u 584524)... si ça donne toujours INVALID, pas de panique, on ressort puis on rerentre dans SoftIce, et on recommence jusqu'à voir quelque chose qui ressemble à :

```
584524 PUSH EBP
584525 ...
```

Nous y voilà, c'est le début du programme ! Mettons-y un breakpoint (pour l'arrêter à son début à la prochaine exécution). Cela se fait en théorie par la commande SoftIce suivante :
bpx 584524 (breakpoint au moment de l'exécution à cette adresse)
Mais sur mon système, cela marche mieux avec :
bpm 584524 x (ce qui fait la même chose)
Un petit "bl" (affiche la liste des breakpoints) permet de vérifier qu'il est bien présent. Maintenant, si on sort de SoftIce, qu'on quitte Toto et qu'on le relance, le programme s'interrompt et on peut voir ses premières instructions, en l'occurrence :

```
0167:00584524 PUSH    EBP
0167:00584525 MOV     EBP,ESP
0167:00584527 PUSH    FF
0167:00584529 PUSH
005C22E0
0167:0058452E PUSH
0058C4FC
0167:00584533 MOV
EAX,FS:[00000000]
0167:00584539 PUSH    EAX
0167:0058453A MOV
FS:[00000000],ESP
0167:00584541 SUB     ESP,58
0167:00584544 PUSH    EBX
0167:00584545 PUSH    ESI
0167:00584546 PUSH    EDI
0167:00584547 MOV     [EBP-
18],ESP
0167:0058454A CALL
[005B5244]
0167:00584550 XOR     EDX,EDX
```

L'Assembleur tu apprendras

Si vous n'êtes pas familier avec l'assembleur, ce que je vais supposer puisque cet article s'adresse à tous, vous devez vous demander ce que ce programme peut bien vouloir dire. Je vais donc vous introduire les principes de base de l'assembleur, de manière très superficielle. Le programme ci-dessus est le listing en assembleur du début du jeu. L'assembleur est le langage de plus bas niveau qu'il existe : c'est celui que le processeur est capable d'exécuter (chaque ligne correspond à une instruction du processeur, est codée en mémoire sur un certain nombre d'octets). Lorsque

Coucou, c'est la RIAA!

Dans sa lutte anti-piratage, la RIAA a manifestement choisi entre la carotte et le bâton... en faveur du bâton. Elle a lancé début mai une campagne de menace "on-line", qui utilise les systèmes de chat intégrés dans les logiciels P2P pour prévenir l'utilisateur qu'il enfreint la loi et qu'il s'expose à des poursuites. Elle compte envoyer ainsi au moins 1 million de messages par semaine, afin de dégoûter les internautes des réseaux P2P. Extraits du message: "Vous semblez partager de la musique sur votre ordinateur (...) Distribuer ou télécharger de la musique protégée par le droit d'auteur est illégal (...) Vous vous exposez à des poursuites (...) Ne volez pas de musique (...) Vous n'êtes pas anonymes sur ces réseaux: vous pouvez facilement être identifiés", etc, etc.. Evidemment, la RIAA ne va pas poursuivre 1 million d'internautes par semaine, l'objectif avoué est avant tout de faire peur. Cela dit, ça ressemble fort à du spam tout ça, ça serait amusant qu'ils se prennent un procès pour violation de la licence d'un logiciel P2P qui interdirait d'envoyer trop de messages.

La fin du monde dans 57 ans!

Je sais, c'est un peu hors-sujet, mais je préfère vous prévenir à l'avance: la fin du monde est prévue pour 2060. Ca vous laisse un peu de temps pour vous préparer. C'est Newton (celui à la pomme), qui en est arrivé à ces conclusions après des années et des années d'étude minutieuse des écrits bibliques. Autant vous dire que ce n'est pas des bobards... Ma seule crainte, c'est que 57 ans c'est beaucoup, j'ai peur d'oublier entre temps et de me faire surprendre. Quelqu'un pourra envoyer un mail au journal pour me le rappeler?

1:1, il faudra donc attendre les prolongations

Le flou juridique entourant le Peer-to-Peer est en train de s'éclaircir un peu outre-Atlantique, avec deux jugements qui pourraient avoir des conséquences importantes pour tous les réseaux P2P. Tout d'abord, le cas de Verizon a enfin été tranché. Rappelons que Verizon était opposé à la RIAA, qui désirait obtenir l'identité de deux internautes soupçonnés d'avoir partagé illégalement des fichiers musicaux via Kazaa. Verizon, leur fournisseur d'accès à internet, dénonçait la requête de la RIAA comme abusive. Finalement, Verizon devra s'exécuter: ce jugement fait peur aux FAI, qui craignent maintenant que n'importe qui se prétendant détenteur d'un copyright puisse obtenir l'identité d'un internaute. Si ce jugement fait évidemment plaisir à la RIAA, une autre décision de justice leur a fait perdre leur grand sourire: les compagnies derrière Grokster et Morpheus ont en effet été jugées non responsables des échanges illégaux de fichiers sur les réseaux. La RIAA ayant bien sûr fait appel, attendez quand même un peu avant de vous réjouir...

Le retour du Hamster

Oups, de Napster, j'avais mal lu le communiqué de presse. Roxio a en effet affirmé sa volonté de faire revivre Napster de ses cendres avant la fin de l'année. Rappelons que Napster, après avoir été shooté en pleine tête par un juge américain, a vu son cadavre traîné un peu partout, racheté par l'un, réattaqué en justice par l'autre, avant de finalement atterrir chez Roxio. Apparemment, le cadavre commence à pourrir et ils n'arrivent pas à s'en débarrasser: c'est donc un Napster tout neuf (et payant) qui devrait bientôt débarquer.

vous écrivez un programme dans n'importe quel langage, et que vous le compilez pour obtenir un exécutable, il est "transformé" en assembleur (c'est l'étape de compilation), de manière à ce que le processeur puisse l'exécuter. Les crackers n'ont généralement pas le code source du programme, c'est pourquoi ils doivent comprendre l'assembleur, de manière à analyser ce que fait le logiciel (c'est ce que l'on appelle le "reverse engineering") pour pouvoir le cracker.

Quelques points à garder en tête quand on programme en assembleur :
- il n'y a que des instructions et des données très basiques (pas de for, while, d'objets...)
- un peu comme dans le bon vieux Basic, les lignes sont numérotées par leur adresse en mémoire, qui s'écrit sous la forme segment:offset. Sous Windows, on peut oublier le segment, et ne travailler qu'avec l'offset, qu'on assimile à l'adresse.
- il n'y a pas de variables à proprement parler. On stocke les données dans ce que l'on appelle les registres. Sur nos machines modernes, un registre peut stocker 32 bits d'information (il tient donc sur 4 octets). Les registres qu'on utilise à cet effet sont nommés EAX, EBX, ECX, EDX. Lorsqu'on a besoin de stocker des données de manière durable, vu le nombre limité de registres, on les stocke plutôt à une adresse mémoire bien choisie.
- il existe des registres ayant des fonctions spéciales. Notamment le registre EIP qui contient toujours l'adresse de la prochaine instruction du programme à exécuter. Le registre ESP, lui, pointe toujours sur l'adresse de la pile : la pile est une zone mémoire utilisée pour stocker des données temporaires. On peut y déposer une valeur (instruction PUSH), et y récupérer la dernière valeur déposée (instruction POP).

Bon, maintenant que vous savez un peu à quoi vous attendre, examinons le programme pas à pas :

```
0167:00584524 PUSH   EBP
```

Oh, je n'ai pas encore parlé du registre EBP ! Il s'agit du registre couramment utilisé pour accéder aux arguments d'une fonction. Comme il va être modifié dans l'instruction suivante, on commence par le sauvegarder sur la pile

```
0167:00584525 MOV    EBP,ESP
```

L'instruction MOV, absolument indispensable, correspond à l'affectation. Sa syntaxe est : MOV destination, valeur. On voit donc qu'ici, on affecte à EBP la valeur d'ESP, c'est-à-dire l'adresse de la pile. C'est classique pour une fonction, qui va chercher ses arguments dans la pile, justement !

```
0167:00584527 PUSH   FF
0167:00584529 PUSH   005C22E0
0167:0058452E PUSH   0058C4FC
0167:00584533 MOV    EAX,FS:[00000000]
0167:00584539 PUSH   EAX
0167:0058453A MOV    FS:[00000000],ESP
```

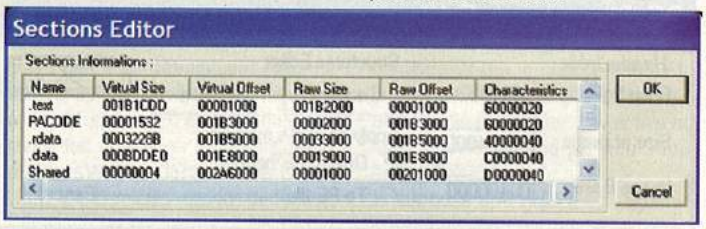
Ici on prépare l'appel à une fonction (le CALL de l'avant-dernière ligne) en stockant un certain nombre de paramètres sur la pile : inutile de chercher à comprendre le sens des valeurs stockées, cela ne nous intéresse pas. Pour ce qui est des instructions MOV, on en verra des un peu semblables, mais plus simples, juste après.

```
0167:00584541 SUB    ESP,58
```

L'instruction SUB permet de soustraire une valeur à un registre. Ici, cela revient à écrire en C : ESP = ESP - 0x58; (le 0x indique qu'il s'agit d'un nombre hexadécimal). Au fait, à ce point, je considère que vous comprenez l'hexadécimal ! Petit truc : la calculatrice de Windows, en mode scientifique, fait la conversion entre hexadécimal et décimal.

```
0167:00584544 PUSH   EBX
0167:00584545 PUSH   ESI
0167:00584546 PUSH   EDI
```

On stocke sur la pile certains registres... Inutile de s'attarder sur ESI et EDI, ce sont juste deux autres registres un peu spéciaux.




```
0167:00584547 MOV    [EBP-18],ESP
```

Encore un MOV, mais un peu différent. Les crochets [xxx] représentent le contenu de l'adresse xxx ! Ainsi, MOV [EBP],ESP stocke la valeur de ESP (4 octets) à l'adresse mémoire EBP (si par exemple EBP est égal à ESP, cela revient à écraser la dernière donnée sur la pile par l'adresse de la pile), et non pas dans le registre EBP !! Ici, MOV [EBP-18],ESP signifie que ESP est stocké à l'adresse EBP moins 0x18 octets. Beaucoup d'instructions autorisent l'emploi de crochets. Vous pouvez par exemple faire : PUSH [ESP] pour stocker sur la pile la valeur à l'adresse ESP, ce qui aura pour effet de dupliquer la dernière donnée de la pile.

```
0167:0058454A CALL   [005B5244]
```

C'est ce qui nous intéresse ! L'instruction CALL sert à appeler un sous-programme. La syntaxe est : CALL adresse. Ici, le programme ne va pas sauter à l'adresse 5B5244, comme vous pourriez le penser, mais à l'adresse dont la valeur est stockée à l'adresse 5B5244, comme vous l'auriez deviné si vous aviez lu un peu plus attentivement ce que j'ai dit juste au-dessus. Mais quelle est donc cette adresse ?

Sa majesté Herr Data

Ok, on va arrêter l'assembleur 5 minutes, et examiner un peu ce qu'on a sous la main. On sait (enfin, on va supposer qu'on le sait) que le fichier Toto.icd est notre exécutable, encrypté. Cela dit, il n'est pas totalement encrypté, et on peut l'analyser avec un éditeur (comme ProcDump). Vous vous rappelez qu'on a utilisé le "PE Editor" au début ? Pourquoi ? Parce qu'un exécutable sous Windows est appelé un fichier PE, pour "Portable Executable". Un fichier PE est structuré d'une certaine manière, en gros avec au début un header qui décrit entre autres les différentes sections du fichier, puis les sections proprement dites. Ces sections contiennent plusieurs choses, notamment le code du programme, mais aussi... les adresses des fonctions importées par le programme, dans la section appelée ".rdata". En effet, il utilise des fonctions de Windows (dans des DLL comme Kernel32.dll ou User32.dll), et les adresses de ces fonctions sont déclarées dans le .rdata. Vous allez voir, vous allez bientôt comprendre.

Relançons ProcDump, et PE-Editons Toto.icd. Puis cliquons sur "Sections", pour voir les sections :

Intéressons-nous pour commencer uniquement à .rdata. On note dans un coin que son "Virtual Offset" est 1B5000, et sa "Raw Size" 33000. A partir de ces informations, comment la récupérer ? Et bien, tout d'abord, il faut un programme pour dumper cette section, pour cela on va utiliser IceDump (mais ProcDump devrait en être capable également). On relance Toto.exe, il s'arrête sur son OEP, et là nous allons sauvegarder la section .rdata sur le disque. Avec IceDump, cela se fait par : pagein d "Virtual Offset + Image Base" "Raw Size" nom_du_fichier

Par exemple ici : pagein d 5b5000 33000 c:\rdata.bin

Il est conseillé de désactiver les breakpoints d'abord (instruction bd, et son contraire be pour les réactiver). Sinon le dump peut être corrompu.

Quittons SoftIce et Toto, et ouvrons rdata.bin avec HexWorkshop, ou tout autre éditeur hexa. Oui, c'est incompréhensible... mais réfléchissons un peu. On s'était arrêté dans notre programme à l'instruction CALL [5B5244].

Or, 5B5244 = 5B5000 + 244, donc l'adresse 5B5244 est à l'offset 244 de notre fichier! Vérifions : dans HexWorkshop, Ctrl-G permet d'aller à l'offset 0x244, et on voit la valeur suivante: 981BE400. Maintenant, si on relance Toto, et qu'on trace le programme jusqu'au CALL (utiliser la touche F8 pour exécuter une instruction à la fois)... juste après le CALL, on se retrouve à l'adresse : 00E41B98. Un problème ? Non, pas du tout, pour une question de poids fort et de poids faible qui importe peu, sachez que toutes les valeurs 16 et 32 bits sont stockées "à l'envers" en mémoire (enfin, les octets sont inversés).

En quoi tout ceci est-il intéressant ? Et bien, l'adresse E41B98 correspond à une fonction de la librairie dplayerx.dll, qui est caractéristique de SafeDisc. Et que fait cette fonction ? Voyons voir le code... attention, c'est ici que les versions de SafeDisc se démarquent en particulier. Dans la version simple, ça ressemble à ça :

```
PUSHAD
PUSH 70
PUSH 00
CALL [E41BB4]
ADD ESP,8
POPAD
JMP [E41BB8]
```

Tout d'abord, PUSHAD équivaut à faire un PUSH de tous les registres, cela permet de tous les sauver en une seule instruction. POPAD permet ensuite de tous les récupérer.
Il faut comprendre que ce petit bout de code va en fait appeler une fonction de Kernel32.dll, en l'occurrence celle numérotée par "70". Plus précisément, le PUSH 70 indique qu'on cherche l'adresse de la fonction numéro 70, puis le PUSH 00 qu'il s'agit de Kernel32.dll (il y aurait un PUSH 01 pour User32.dll). Ensuite, la fonction dont l'adresse est stockée en E41BB4 est appelée (les deux PUSH servent donc à stocker ses paramètres). Cette fonction est propre à SafeDisc, qui va se débrouiller pour retrouver la bonne adresse de la fonction désirée dans Kernel32 ou User32, et va la stocker... à l'adresse E41BB8 !! Quand on arrive à l'instruction JMP [E41BB8], on saute donc dans une dll Windows (JMP est l'instruction permettant d'aller à une adresse précise), à la suite de quoi on revient là où le dernier CALL a eu lieu... c'est-à-dire sur l'instruction 0167:00584550 XOR EDX,EDX (du début de notre programme).

Vous comprenez ce que fait SafeDisc? Il remplace les adresses de certaines fonctions de Kernel32.dll et User32.dll dans .rdata par des adresses vers ses propres routines, qui peuvent vérifier le cd ou faire plein d'autres choses indésirables... C'est pour cela que si on se contente de dumper le programme entier avec IceDump une fois qu'il a été décrypté, il plantera dès le premier CALL. Toute l'astuce consiste donc à récupérer les bonnes adresses pour reconstruire la section .rdata, afin de ne plus appeler les fonctions de SafeDisc.

Merci SafeDisc !

Dans ce cas-ci, la tâche ne va pas être bien compliquée. En effet, on remarque qu'après le code de l'adresse E41B98, on voit un tout petit peu plus loin, à l'adresse E41BC6 = E41B98 + 2E :

```
PUSHAD
PUSH 71
PUSH 00
CALL [E41BE2]
ADD ESP,8
POPAD
JMP [E41BE6]
```

Et ainsi de suite : tous les 2E octets, une nouvelle fonction, la prochaine aura PUSH 72, etc... si on descend encore, on arrive à la fonction numéro 89, puis ensuite on a le bout de code à l'adresse E42044 :

```
PUSHAD
PUSH 00
PUSH 01
CALL [E42060]
...
```

On commence donc ici les appels vers les fonctions de User32.dll ! Si on en cherche la fin, on arrive finalement à la fonction numéro 49 de User32, il y a donc 4A appels au total (et 8A dans Kernel32). Ce nombre d'appels, ainsi que les adresses, varient évidemment selon le jeu. En plus, on se rend vite compte que le CALL [xxxx] appelle toujours la même fonction : il va donc nous suffire de l'appeler avec tous les numéros possibles de fonctions (de 0 à 89 pour Kernel32, et de 0 à 49 pour User32), et le tour sera joué ! Enfin, si on trace le programme à partir du début avec F8 jusqu'en E41B98, puis avec F10 (permet de tracer sans rentrer dans les appels de fonction) jusqu'au ADD ESP,8 (on ne rentre pas dans la fonction qui calcule la bonne adresse), on se rend compte que la valeur à l'adresse E41BB8 (donc la bonne adresse) est aussi celle du registre ECX ! (SoftIce affiche en permanence les valeurs des registres, en haut, et pour voir la valeur de l'adresse E41BB8, il suffit de faire d E41BB8). Et la valeur de EAX est aussi la "mauvaise" adresse (E41B98), c'est-à-dire l'adresse présente dans la section .rdata. Attention, avec les versions plus récentes de SafeDisc, ça s'est un peu compliqué, mais on verra ça plus tard...

Nous allons donc coder notre propre programme en assembleur pour corriger la section .rdata. On relance Toto et on s'arrête au début, puis on copie la section .rdata dans une zone accessible en écriture (on ne peut pas écrire directement sur .rdata), par exemple .data (zone contenant les données du programme). Manque de bol, .rdata est plus gros que .data dans notre cas ! mais en fait seul le début de .rdata a besoin d'être corrigé, donc on peut se contenter des 0x10000 premiers octets par exemple. On réalise la copie ainsi dans SoftIce:

Le miel attire le hacker

Comment attraper un hacker? Avec du miel! Il existe en effet des ordinateurs pièges, appelés "honeypots" (pots de miel) en anglais, mis en ligne par des spécialistes de la sécurité informatique pour attirer le hacker imprudent. Ces "honeypots" peuvent par exemple faire semblant d'être vulnérables à une certaine faille (en envoyant une fausse réponse à un programme de scan), pour encourager un hacker à s'y attaquer. Ou bien, ils servent simplement à analyser les techniques employées par les hackers pour pénétrer dans un système, afin de découvrir des failles de sécurité qui n'ont pas encore été publiées. Une autre technique consiste à camoufler de fausses informations "confidentielles" qui déclenchent l'alarme lorsque quelqu'un y accède (appelées des "honeytokens"). Un programme de contrôle sniffe le réseau, et s'il voit passer un tel fichier, il alerte l'administrateur. Bref, les apprentis-hackers feraient bien de se méfier, les proies alléchantes que semblent être certains ordinateurs sur le net peuvent en fait n'être que des leurres!

Le clic droit qui tue

Un joli petit bug tellement débile qu'on se demande comment il a pu rester inaperçu si longtemps a été découvert sous XP: un clic droit sur un fichier dans l'explorateur provoque une utilisation de 100% du processeur! Microsoft a reconnu le bug, mais ne compte pas le corriger, car il faudrait toucher à trop de composants critiques du système d'exploitation. Pour éviter ça, vous pouvez soit faire d'abord un clic gauche sur le fichier, soit désactiver l'effet de transition dans l'onglet Apparence des options d'affichage, bouton "Effets".

m 5B5000 l 10000 5E9000

J'ai pris 5E9000 au lieu de 5E8000 (le début de .data) pour prendre un peu de marge, mais ça ne devrait pas faire de différence.

Bien. Ne reste plus qu'à écrire un petit programme. Dans SoftIce, on peut écrire en assembleur à partir d'une adresse en tapant "a adresse". Etant positionné sur le point d'entrée, on peut utiliser "a eip", qui permet de commencer à écrire en assembleur à partir de l'instruction courante. Le listing du programme qu'on veut écrire, est, en notation un peu allégée (avec des labels pour représenter les adresses importantes) :

```
MOV EBX,00  // on stocke dans EBX 0 ou 1 (pour Kernel32 ou User32)
Debut_Librairies:
MOV EDX,00  // on stocke dans EDX le numéro de la fonction
Debut_Fonctions:
PUSH EDX// passage des paramètres de la fonction de SafeDisc
PUSH EBX// (d'abord le numéro de fonction, puis de librairie)
CALL 904990  // appel de la fonction de SafeDisc
PUSH EDX  // on sauvegarde EDX sur la pile pour la suite
MOV EDX,5E9000  // EDX pointe sur le début de notre copie de .rdata
Scanne_Rdata:
CMP DWORD PTR [EDX],EAX
        // est-ce qu'on a dans .rdata la valeur de EAX ?
JZ Remplace
        // si oui, on va la remplacer par la bonne
ADD EDX,4  // si non, on continue de scanner le .rdata
CMP EDX,5E9000 + 10000
  // a-t-on fini de scanner le .rdata ?
JNZ Scanne_Rdata
  // si non, on continue
JMP EIP
  // si oui, on bloque ici ! (ce n'est pas normal)

Remplace:
MOV DWORD PTR [EDX],ECX
        // on met dans le .rdata la bonne adresse (ECX)
POP EDX  // on récupère le numéro de fonction sauvé
INC EDX  // passage à la fonction suivante...
CMP EBX,0  // travaillons-nous sur Kernel32.dll ?
JNZ User32  // si non, on saute
CMP EDX,8A  //si oui, avons-nous fait déjà 8A fonctions?
JNZ Debut_Fonctions
        // si non, on continue avec la prochaine
INC EBX  // si oui, on passe à User32.dll
JMP Debut_Libraries  // et on recommence !
User32:
CMP EDX,4A  // avons-nous déjà fait 4A fonctions ?
JNZ Debut_Fonctions  // si non, on continue
JMP EIP  // si oui, on s'arrête ici !
```

Ce petit programme nous permet de voir quelques instructions supplémentaires en assembleur :

- CMP x,y sert à comparer deux valeurs. Si elles sont égales, le "flag" Z est mis à 1, sinon il est mis à 0. Un flag est un bit stocké par le processeur, qui peut être modifié et testé par certaines instructions.
- JZ ou JNZ est l'instruction classique qui suit un CMP. JZ signifie "Jump if Zero", c'est-à-dire, fait un saut si le flag Z est à 1, tandis que JNZ fait le contraire (saute si le flag Z est à 0).
- INC x permet de rajouter 1 à x. Ainsi, INC EDX est équivalent à ADD EDX,1 (je suppose que vous aviez compris que ADD permettait de faire une addition !)
- le DWORD PTR utilisé à 2 reprises permet de faire comprendre à SoftIce, quand on tape, qu'on veut utiliser tous les 4 octets d'une adresse précise. Si on ne le met pas, il ne va pas assembler le code désiré. Pour la compréhension du programme, vous pouvez faire comme s'il n'était pas là.

Sous SoftIce, le code ressemble à ça :

```
584524 MOV  EBX,00000000
584529 MOV  EDX,00000000
58452E PUSH EDX
58452F PUSH EBX
584530 CALL 00904990
584535 PUSH EDX
584536 MOV  EDX,005E9000
58453B CMP  [EDX],EAX
58453D JZ   0058454C
58453F ADD  EDX,04
584542 CMP  EDX,005F9000
584548 JNZ  58453B
58454A JMP  0058454A
58454C MOV  [EDX],ECX
58454E POP  EDX
58454F INC  EDX
584550 CMP  EBX,00
584553 JNZ  00584560
584555 CMP  EDX,0000008A
58455B JNZ  0058452E
58455D INC  EBX
58455E JMP  00584529
584560 CMP  EDX,4A
584563 JNZ  0058452E
584565 JMP  00584565
```

On peut sauvegarder son programme à l'aide de IceDump, afin de ne pas avoir à le réécrire en entier plus tard si les choses tournent mal. Ici, on le ferait avec :

`pagein d 584524 42 c:\prog.bin`

(0x42 = la longueur du programme, en octets)

Ensuite, on quitte SoftIce et on laisse tourner... normalement, rien ne doit se passer. Et en retournant dans SoftIce, on doit se retrouver à l'adresse 584565. Si on est en 58455A, cela signifie que le programme a cherché partout dans le .rdata sans arriver à trouver la mauvaise référence (contenue dans EAX) : il y a donc un problème, et tracer le programme à la main pour comprendre ce qui ne va pas s'impose.

Si tout va bien, on a par contre notre nouvelle section .rdata de prête ! Il ne reste plus qu'à la sauvegarder, par :

`pagein d 5E9000 10000 c:\bon_rdata.bin`

'IZ

IL N'Y A PAS D'ÂGE POUR PIRATER

On a peut-être trouvé le hacker le plus jeune de l'Histoire : il s'agit d'un gamin de 11 ans, américain of course. Le petit malin, qui réside en Floride, avait tenté de modifier ses notes de fin de trimestre. La sanction a été sévère : le principal du collège a exigé que le petit soit renvoyé définitivement. En plus de cela, il a dû passer une journée en prison ! La " tolérance zéro " est bien à l'œuvre aux Etats-Unis... Après tout, n'a-t-il pas commis une simple bêtise comme tout autre enfant du même âge ? Ou peut-être avait-il lu Pirat'z ?

VOTRE IP NE SERA PLUS PROTÉGÉE

Ce n'est pas un poisson d'avril, et c'est pourtant le 1er avril que le Sénat a adopté un projet de loi réformant la loi de 1978 sur le traitement des données nominatives. Une réforme qui risque de bouleverser la donne chez les internautes français, puisqu'on y trouve notamment une modification au niveau des personnes susceptibles de collecter des données personnelles. Dorénavant, ce ne seront plus seulement les autorités judiciaires qui seront autorisées à "procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté", mais aussi les "les personnes morales victimes d'infractions", "pour les stricts besoins de la lutte contre la fraude". Traduction pour les adeptes de P2P: des organismes privés luttant contre le piratage pourront stocker les adresses IP d'internautes, ce qui était jusqu'à présent interdit, une IP étant considérée comme une donnée nominative. Le texte doit encore passer devant l'Assemblée Nationale, mais je sens que chez Retspan, on prépare déjà le champagne!

Ensuite, sous HexWorkshop, on ouvre rdata.bin et bon_rdata.bin, on sélectionne le second en entier, et on le colle dans le début du premier... et le tour est joué, le .rdata est corrigé !

Et c'est tout ?

Oui, enfin... presque :) Il reste à reconstruire un exécutable complet. Pour cela, on peut faire une copie de Toto.icd, appelée par exemple Tutu.exe, que l'on ouvre sous HexWorkshop. Ensuite, on copie chacune des sections à leur offset, indiqué dans ProcDump par "Raw Offset". Quelles sections ? Et bien, toutes ! On va toutes les dumper, exactement comme on a fait pour le .rdata au début. Elles sont toutes décryptées et prêtes à l'emploi quand on s'arrête à l'OEP du programme, sauf le .rdata qu'il fallait modifier.

Quand tout ça est fait, normalement on peut tout fermer, et lancer Tutu.exe... et ça marche ! Attention quand même, l'exécutable ainsi obtenu ne fonctionnera que sous le Windows sous lequel il a été cracké, à cause des adresses des fonctions de Windows dans le .rdata, que nous avons mises nous-mêmes alors que Windows préfère les calcule automatiquement au démarrage. Mais, pas de panique, un petit coup de ProcDump, on clique sur "Rebuild PE" (avec les options par défaut ça devrait marcher), et voilà notre Tutu.exe fonctionnel !

Pff, trop facile !

Voilà, ça c'est la théorie, mais ça ne marchera que pour cette version de SafeDisc. En effet, les auteurs de la protection l'ont continuellement modifiée pour rendre le crack plus difficile. Une version très légèrement différente ne renvoie plus les deux valeurs qui nous intéressent dans EAX et ECX. Par contre, elle va toujours mettre la bonne adresse un peu après chaque fonction dans dplayerx.dll (0x20 octets plus loin, par exemple en E41BB8 pour la fonction qu'on a vue en E41B98). On peut alors facilement adapter le programme, qui ira lui-même chercher les bonnes valeurs. En gros, cela donnerait un bout de code de ce genre, avec EDX contenant le numéro de fonction, et pour les imports de Kernel32.dll :

```
MOV EAX,EDX
IMUL EDX,2E
   // multiplication par la taille de
      chaque fonction
ADD EAX,E40778
  // E41B98-2E*70, la première
     "mauvaise" adresse de Kernel32
```

A ce moment, EAX contient l'adresse à remplacer dans le .rdata, et on peut faire comme avant. Pour récupérer dans ECX la bonne adresse à mettre, ça va ressembler à :

```
MOV ECX,[EAX+20]
```

Et ce n'était pas beaucoup plus compliqué !

Mais ce n'est pas tout. Une autre variante n'utilise plus le JMP qui suit l'appel à la fonction de SafeDisc qui trouve la bonne adresse (on s'en rend compte en traçant le programme, qui n'arrive jamais jusqu'au JMP) : l'appel à la fonction de Kernel32 ou User32 est effectué directement dans cette fonction, ce qui empêche en théorie de l'appeler aveuglément avec toutes les combinaisons de librairie et de numéro de fonction. Pour contourner cette protection, il faut d'abord analyser la fonction, puis la modifier (en mémoire) pour qu'elle n'appelle plus les fonctions systèmes, et ensuite on peut l'utiliser comme avant. Enfin, une des dernières améliorations à SafeDisc 1 est plus subtile : la fonction système appelée par la fonction SafeDisc peut varier selon qui appelle ! C'est-à-dire qu'à chaque 'fausse" entrée dans notre .rdata, peuvent correspondre plusieurs adresses... dans ce cas, on ne peut plus se contenter de ne modifier que le .rdata, il faut aussi aller toucher au programme pour appeler les bonnes fonctions aux bons endroits, et ça devient plus compliqué.... Bah, ça nous fera un challenge à surmonter pour le prochain numéro !

LA BASE DE L'HEXADÉCIMAL

Si vous n'avez jamais vu d'hexadécimal (ou hexa pour les intimes) dans votre vie, vous allez être un peu dérouté, vu que presque tout est en hexa dans l'article. En effet, c'est une manière d'écrire les nombres plus proche de leur représentation par l'ordinateur. La base, c'est facile, c'est la base 16, c'est-à-dire que les unités ne vont plus de 0 à 9, mais de 0 à 15. Et pour les représenter avec un seul caractère, on utilise les lettres, ce qui donne : 0,1,..,9,A,B,...,F. Ensuite, 10 en hexa vaut 16 dans notre système numérique classique, 11 vaut 17, ... 1F vaut 1*16 + 15 = 31, ... jusqu'à FF = 255, puis on continue : FF + 1 = 100 en hexa = 256 en décimal, ..., FFFF = 65535, etc. Facile !

IZ

Le Clone Clone

Si vous vous intéressez un tant soit peu à la copie CD, vous n'avez pas pu passer à côté de CloneCD, le célébrissime copieur capable de dupliquer une bonne partie des protections existantes. Depuis peu, on trouve aussi sur le marché un logiciel appelé CloneDVD, qui n'a en fait rien à voir avec le CloneCD original! Il s'agit d'une tentative assez misérable pour tromper les consommateurs en profitant de la popularité de CloneCD. Je vous conseille donc de l'éviter, après tout ce ne sont pas les logiciels de copie de DVD qui manquent.

Shareaza bientôt maître du monde

On en parle peu car il est moins populaire que les plus gros, mais le réseau Gnutella est quand même un des poids lourds du P2P, et il continue tranquillement son petit bonhomme de chemin. Les nouveaux venus seront peut-être surpris de voir qu'il existe également un Gnutella 2, qui coexiste avec le Gnutella original. Pourquoi? En fait, le soi-disant "Gnutella 2" n'est pas approuvé par les créateurs d'origine de Gnutella. Il s'agit d'un protocole propriétaire développé par le programmeur de Shareaza, un des clients Gnutella (Gnutella est le nom du protocole, il existe plusieurs clients compatibles, comme BearShare et LimeWire). Shareaza est donc considéré comme un client abusif par les développeurs Gnutella, voulant se faire un nom en profitant de Gnutella. Et apparemment ce n'est pas fini, puisque Shareaza, dans sa mégalomanie, est dorénavant également compatible avec Overnet/eDonkey et DirectConnect. Est-ce une bonne nouvelle? C'est à voir, la qualité de l'implémentation des protocoles de ces deux réseaux étant primordiale pour en juger.

COPIER SES

SUITE DU PIRAT'Z N°2

SAUVEGARDER ARMY MEN : SARGE'S HEROES 2

AUX ARRÊTS!

On vous avez conté comment des militaires américains avaient été pincés par la RIAA en flagrant délit de distribution de films et de MP3 via le réseau de la base. C'est qu'ils en profitaient bien de leur connexion à 100 Mbits, les petits veinards! Et bien, les sanctions sont tombées. Au lieu d'être fusillés, les 85 coupables seront systématiquement assignés au lavage des toilettes et n'auront pas leur médaille de la défense nationale. Trop dur, quand on pense qu'un étudiant pincé pour la même raison devra s'acquitter de 15000$...

DEVIANCE REMPORTE LA COURSE

Les protections CD évoluent, et posent continuellement de nouveaux challenges aux groupes pirates. Même si pour l'instant aucun jeu ne semble être parvenu à déjouer les meilleurs crackers, TOCA Race Driver leur a manifestement donné quelques maux de tête. Pas moins de 3 groupes ont sorti leur version crackée. Tout d'abord, FAIRLiGHT, le 26 mars. Mais le lendemain, iMMERSiON sortait une version "Proper" (corrigeant les problèmes de celle de FAIRLiGHT). En effet, ils se sont aperçus que le jeu avait tendance à rebooter tout seul, que les contrôles s'inversaient au bout d'un certain temps, et que l'IA des conducteurs se mettait aussi à déconner. Pourquoi? A cause de la protection (SecuROM), assez poussée dans ce cas-là. Mais ce n'est pas fini: le jour d'après, DEViANCE sortait une version "Real Proper" (c'est-à-dire corrigeant vraiment tous les problèmes): même dans la version d'iMMERSiON, des choses bizarres arrivaient, comme des voitures qui s'envolaient! Enfin, l'honneur est sauf, apparemment cette 3ème tentative a été la bonne et la protection a été annihilée...

VOUS DEVEZ APPRENDRE A RECONNAITRE LES DVD CHECKS

[PRÉSENTATION :]

Pour cette suite des leçons du Pirat'z numéro 2, nous allons voir comment faire tenir un jeu sur un CD en enlevant les fichiers vidéo. Ici, nous utiliserons un fichier film du DVD pour remplacer ceux que nous effacerons, et nous rencontrerons aussi dans le code hex un " DVD check ". Si vous ne savez pas ce que c'est, alors, vous avez sauté une étape de la leçon 2 :).

[ETAPE 1]

Mettre votre DVD dans le lecteur DVD. Faire un répertoire temporaire sur votre disque dur et copier tous les fichiers et répertoires du DVD dans celui-ci. Regarder s'il y a un nom de volume pour le DVD.

[ETAPE 2]

Encore une fois, il va falloir regarder la taille totale des fichiers. Les sélectionner tous, clic droit et " Propriétés". Trop grand pour rentrer sur un CD, il va falloir ripper quelque chose. Si vous regardez dans le répertoire FMV, vous verrez quelques fichiers .PSS. Comme dit dans la leçon 1, ce sont des fichiers de film, faciles à ripper. Vous verrez que le plus petit PSS est m01.PSS. Maintenant, enlever un certain nombre de gros fichiers .PSS, juste assez pour que la taille totale du jeu soit en dessous de 700MB. Prenez ensuite le fichier m01.PSS et faites des copier/coller avec lui, en le renommant avec le nom des fichiers que vous avez effacés. Vous devriez de nouveau avoir tous les fichiers de jeu.

[ETAPE 3] LE DVD CHECK

Ouvrir Hex Workshop et le fichier SLUS de Sarge's Heroes. Il devrait se nommer : SLUS_201.32. Presser Ctrl+F et faire une recherche pour la chaîne hex suivante : 02000424. Il y en a plusieurs instances. Dans la première leçon, nous avons vu quelques chaînes qui n'étaient pas les bonnes. Jetez un coup d'œil dessus et regardez si vous ne pouvez pas voir quelques-unes qui étaient dans cette leçon. Astuce : si la chaîne se trouve dans la deuxième moitié du SLUS ou plus loin encore, ce ne sera sûrement pas celle que vous recherchez. Eliminez-les ;). Maintenant, observez un petit peu cette exemple d'un chaîne correcte : 0000 9886 [8293] 0600 [40]10 0100 0424 8CC4 040C [02]00 0424.

Les chaînes dans les [] sont les chaînes importantes. Ces chaînes permettent, en gros, de vérifier de quel média il s'agit. Elle équivaut à : " si ce n'est pas le bon média, alors arrête la lecture ". Si vous changez le [02] en [01], alors la chaîne se transforme en : " si ce n'est pas le bon média, peu importe, continue de lire ".

Le codage de cette chaîne dépend du développeur du jeu, donc cette chaîne ne sera pas la même d'un jeu à l'autre. Cependant, la chaîne importante (0200 0424) n'a jamais changé jusqu'ici du moins. C'est pourquoi il faut rechercher 0200 0424 au début. Le problème est qu'il y a quelques fois beaucoup d'instances de cette chaîne. Alors, comment savoir laquelle changer ? Malheureusement, il n'y a pas de méthode miracle. Vous devez apprendre à reconnaître les similitudes avec d'autres " DVD check " valides, aussi bien que de reconnaître à quoi ressemblent les mauvaises chaînes.

- La chaîne à changer est celle-ci :

A012 0100 0424 1300 D516 [02]00 0424 0100 0424 D25F

Elle se trouve à Offset:00018C94. Si vous regardez de près, vous verrez les similitudes avec la chaîne plus haute en exemple. Comme dans notre premier exemple, vous voyez que la chaîne que nous voulons est précédée par 0100 0424 xxxx xxxx. Aussi, vous pouvez constater qu'il n'y a seulement qu'une instance de cette chaîne dans tout le fichier. Il n'y a en temps général qu'une seule fois la chaîne du " DVD check ". Maintenant, pressez Ctrl+H pour vous obtenir la boîte de dialogue " Replace " de Hex Workshop. Dans la première ligne, il faut entrer : A012010004241300D51602000424, et dans la seconde, la chaîne corrigée: A012010004241300D51601000424.

Vous pouvez voir que le 02 sera remplacé par 01. Presser OK et Hex Workshop s'arrêtera à la première chaîne trouvée, en vous laissant le choix de faire ce que vous voulez. Vu que nous savons que cette chaîne n'apparaît qu'une fois, sélectionner " Replace All." Vous recevez alors un message disant qu'une chaîne a été remplacée. Maintenant, enregistrer le fichier et quitter Hex Workshop.

[ETAPE 4]

Ouvrir CD\DVD Generator et choisir " Create New Project ", " CDROM Master Disc ". Vous arrivez à la fenêtre DIRECTORY. Cliquer sur VOLUME en entrer le nom de disque dans " Disc Name " sous " Master Disc ". Comme toujours, c'est le nom de votre fichier SLUS. Ici, ce sera normalement SLUS20132. Maintenant, cliquez sur DIRECTORY. Vous allez créer vos répertoires. Pour ce jeu, il y a quelques-uns. Créer d'abord tous les répertoires principaux, puis les sous-répertoires. NOTE : pour créer un sous-répertoire, sélectionner d'abord le répertoire dans lequel il doit être, puis sélectionner " Create Directory ". Une fois que tous les répertoires ont été faits, vous êtes prêts pour la suite.

[ETAPE 5]

Comme dans la leçon 1, ouvrir ISOBuster pour regarder l'ordre des fichiers. Comme avant, faire glisser les fichiers dans CD\DVD Gen dans l'ordre indiqué par ISOBuster. NOTE : pour mettre un fichier dans un dossier, vous devez d'abord sélectionner ce dossier dans CD\DVD Gen. L'icône se changera en un dossier ouvert si vous l'avez fait correctement. Mettre tous les fichiers dans le bon ordre et dans le bon répertoire. Cela fait, vous pouvez faire votre fichier iml comme tout à l'heure. Le nommer le sarge.iml et le mettre dans le même répertoire que IML2ISO.EXE. Fermer CD\DVD Gen and ISOBuster.

[NOTE:] Encore une fois, pour ceux parmi vous qui utilisent un système de swap sans modchip, vous pouvez placer SYSTEM.CNF au LBA 12231. Si votre image devient alors trop

JEUX PS2

grosse, créer un " DVD Master Disc Project " au début.

[ETAPE 6]
A partir de DOS, ou de Démarrer/Exécuter..., Faites comme pour le jeu précédent : " iml2iso nom-dujeu.iml NOMDUJEU.ISO ". Une fois cela fait, vous pourrez effacer les fichiers du répertoire temporaire.

[ETAPE 7]
Prêt pour graver ! Procéder comme dans le Pirat'z 2, avec les même options.

Vous venez de faire votre second DVD Rip ! Vous devriez maintenant être à l'aise avec les procédés utilisés. Vous connaissez maintenant différents moyens de remplacer des fichiers et de contourner le " DVD Check ". Pour notre prochaine leçon, nous allons aborder un jeu plus difficile : Summoner.

ET POUR FINIR : SUMMONER

[PRÉSENTATION :]
Vous allez voir comment éditer et effacer des fichiers autres que des .pss, ce que tout bon " rippeur " doit savoir faire.

[ETAPE 1]
Tout d'abord, copier tous les fichiers sur le disque dur. Sauf music.vpp, demo.pss, et geeks.pss, que l'on rippe.

[ETAPE 2]
Il va falloir " remplacer " les fichiers rippés. Dans cet exemple, THQLOGO.PSS , copié puis renommé en GEEKS.PSS et DEMO.PSS. Vous remarquerez un fichier dans ce jeu nommé MUSIC.VPP. Comme vous l'aurez certainement deviné, c'est un fichier de musiques. Il va falloir tout simplement effacer MUSIC.VPP puis créer un " dummy file " de 1Mo ou simplement faire un fichier texte de 0ko, puis renommer cela en MUSIC.VPP. Ouvrer alors le fichier SLUS dans Hew Workshop et faire une recherche rapide pour MUSIC.VPP. La voici. Effacer la référence et la remplacer par un nombre équivalent de 00.
EXEMPLE :

MUSIC.VPP <-- original
..... <-- après modif.

Tant que vous y êtes, regardez s'il n'y a pas de " DVD check " en cherchant la chaîne 02000424. Vous verrez qu'il y a beaucoup d'instances trouvées. Mais après examen, il s'avère qu'aucune d'elles n'est un " DVD Check " !

[ETAPE 3]
Vous êtes prêt pour DVD Gen. L'ouvrir et créez une liste de fichiers en sélectionnant " iso " sur la fenêtre de gauche ", puis en faisant un clic droit et en sélectionnant " Copy Tree-Info to File. "

Maintenant allez dans VOLUME, entrez SLUS20040 et exportez le fichier iml file.
Au cas où il y a un nom de volume pour le DVD, l'entrer aussi.

[NOTE:] Comme avant, vous pouvez placer SYSTEM.CNF au LBA 12231 pour utiliser une méthode de swap sans modchip.

[ETAPE 4]
Aller sous DOS ou dans Démarrer\Exécuter... et entrer : " iml2iso summoner.iml summoner.iso " Effacer alors votre répertoire temporaire.

[ETAPE 5]
Et voilà, il ne vous reste plus qu'à graver de la façon habituelle.

Vous venez de faire un rip de Summoner qui fonctionne parfaitement.
Celui-ci était très simple, mais il vous a montré un nouveau type de fichier que vous pouvez ripper au cas où vous n'obtenez pas assez d'espace en enlevant les fichiers PSS, ce qui est une chose importante à savoir. Il vous a aussi permis de voir quelques mauvaises chaînes de " DVD Check " dans le fichier SLUS, car même si le nombre d'instances trouvé paraît important, cela ne veut pas forcément dire qu'il y a une chaîne valide. Si vous n'avez pas examiné ces chaînes, alors faites-le !

Je vous donne rendez-vous dans le prochain numéro de Pirat'z pour de nouvelles aventures. En attendant, n'hésitez pas à nous envoyer vos commentaires et vos idées.

RÉSULTATS DE NOTRE ENQUÊTE LECTEURS

De sexe masculin. Obsédé par les ordinateurs. Sans petite amie. Agé de 14 à 34 ans. Désireux de foutre le b**** dans le monde entier. Voilà ce que je lis dans votre main, cher lecteur. Ah non, je me trompe, c'est plutôt ce que je lis dans une étude menée par un expert en anti-virus, concernant le profil moyen des créateurs de virus. "Ils sont incapables d'avoir une copine, sont généralement complètement asociaux et sont obsédés par l'idée de créer des virus", dit-il. Et alors? A quoi peut donc servir une telle étude? A repérer les programmeurs de virus parmi vos amis? Voyons, regardez-moi, je n'ai jamais écrit un seul virus, et pourtant, euh, hmm... bon, voilà, quoi. Et puis, publier de telles choses, ça va mettre en rogne ces gens-là, qui vont vouloir montrer que c'est faux, en se trouvant une pauvre fille qui va se retrouver délaissée au profit de l'ordinateur.. En tout cas, si tu es une fille de 18 à 25 ans, que tu n'as pas de copain, et que tu écris des virus, écris donc au journal, j'aimerais t'interviewer pour le prochain numéro ;p

L'EGLISE ENGAGE DES HACKERS

En février dernier, (au moins) un hacker était parvenu à voler plusieurs millions de numéros de cartes de crédit Visa. Le message officiel était: "aucun de ces numéros n'a été utilisé frauduleusement". Ben oui, le hacker voulait juste compléter sa collection personnelle, peut-être ? En fait non puisqu'un soi-disant prêtre nigérian a utilisé un des numéros volés pour une commande de 1686$ à une imprimerie catholique...

LES METIERS DE LA

Voici le premier volet d'une nouvelle rubrique dans Pirat'z : nous allons vous faire découvrir les différents acteurs de la scène pirate, qui sont des personnages de l'ombre très peu (et mal) connus du grand public. Dans chaque numéro, nous allons donc décrire un type de "poste" dans la scène Warez. Et non, inutile d'envoyer vos CV et lettres de motivation au mag', ce n'est pas nous qui embauchons !

WAREZ

IL N'Y A PAS DE VOLEUR HONNÊTE

Le site "The Honest Thief" (Le Voleur Honnête) a fait parler de lui pendant un bon mois en mars. Il annonçait en effet rendre enfin le partage de fichiers musicaux légal, par une idée tout simplement révolutionnaire. Il s'agissait de prendre un peu de puissance CPU sur votre machine, afin de pouvoir faire du calcul distribué. En revendant la puissance de calcul ainsi obtenue, la compagnie propriétaire du réseau était alors capable de rémunérer directement les artistes dont les chansons étaient téléchargées (en éliminant au passage l'intermédiaire des majors). C'est génial hein? Un peu trop génial pour être vrai... pourtant, beaucoup y ont cru et y ont vu la solution aux problèmes du P2P, et le site de la compagnie a ainsi été énormément médiatisé. Jusqu'au 1er avril, où on a appris... hmm, je vous laisse deviner (indice: ça a un rapport avec la date). Tout ça avait en fait été mis en place pour... faire de la publicité pour un bouquin! Pff, moi j'espère que leur bouquin, on va bientôt le retrouver en téléchargement sur le net au format PDF!

FREE FAIT PEUR, PUIS RASSURE

Les abonnées de Free ont eu peur lorsqu'a été publiée sur le net une lettre reçue par un internaute de la part du service "Abuse" de Free. Cette lettre lui reprochait d'avoir téléchargé certains fichiers copyrightés. Oups. Free a rapidement clarifié les choses: ils avaient reçu une plainte de l'IDSA (Interactive Digital Software Association) et s'étaient contenté de la relayer, laissant l'abonné décider seul de ce qu'il en ferait. Enfin, moi, je me serais calmé...

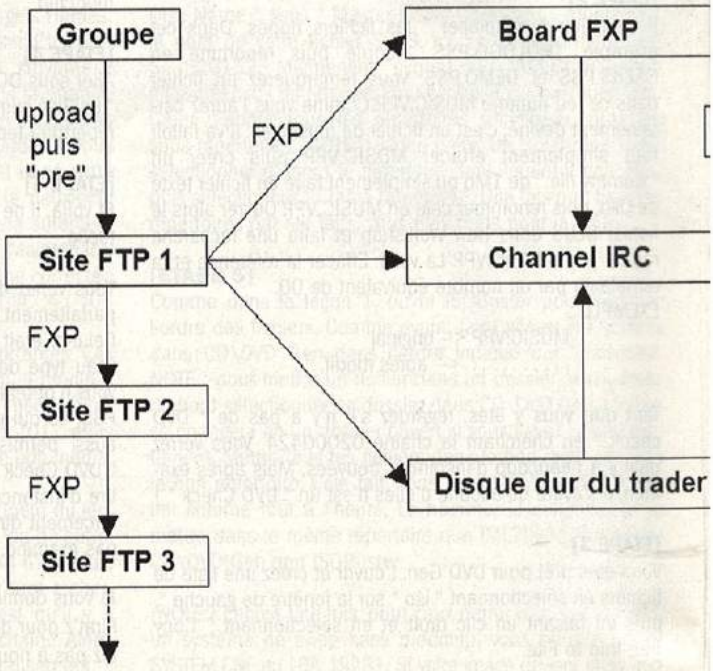
Aujourd'hui, intéressons-nous au métier méconnu de.... siteop. "Siteop" signifie "Site Operator", c'est-à-dire "exploitant de site", si on le traduit littéralement en français. Ce qui ne nous avance pas à grand-chose vous en conviendrez. Mais peut-être faut-il commencer par rappeler les bases du fonctionnement de la Scène Warez, car seuls nos plus fidèles lecteurs doivent encore se souvenir de l'article à ce sujet dans le Pirat'gamez numéro 4.

COMMENT FONCTIONNE LA SCÈNE

Un peu d'histoire donc... en 1911, naquit le groupe Razor, d'où le nom Razor1911. Bon ok, c'était sans doute un peu plus tard, mais bon bref, Razor1911 est un des plus anciens "release groups" de la scène Warez. Un "release group" en anglais, qu'on va simplement appeler "groupe" ici, c'est une petite organisation de membres disséminés de par le monde, dont l'objectif est de cracker avant les groupes concurrents les derniers jeux, utilitaires, ou de ripper les films, mp3, etc... et de les distribuer ("to release" en anglais) sur le net. Si vous voulez voir quelles sont les dernières releases de la Scène et les différents groupes, allez par exemple sur www.nforce.nl
Contrairement à ce que pas mal de monde semble penser, eDonkey et les autres réseaux Peer-to-Peer ne sont pas les premiers à recevoir les releases. Celles-ci sont d'abord distribuées sur de gros serveurs FTP, appelés... tadadam... les sites. Ces serveurs n'ont rien à voir avec le ftp que vous avez installé sur votre adsl, qui culmine à la vitesse vertigineuse de 64/16 ko/s... non, ici on parle de serveurs à minimum 10 Mbits/s (petits sites), et plus généralement 100, 200 Mbits/s ou même 1 Gbit/s pour les gros sites (quant aux sites qui sont sur l'Internet 2 expérimental, je vous laisse imaginer). Pour atteindre de tels débits, ces sites ne sont bien sûr pas hébergés par des particuliers (sauf pour les 10 Mbits/s, qui sont accessibles à des prix raisonnables dans certains pays comme la Suède - avec le provider bbb - mais jusqu'à quel point une telle connexion est-elle utile dans un igloo ?). Ce sont donc les lignes d'entreprises ou d'universités qui sont le plus souvent squattées, évidemment à l'insu du plein gré de celui qui paie la facture internet. Tout ceci pose, vous vous en doutez, pas mal de problèmes de sécurité pour parvenir à camoufler le site, mais on va y revenir...

La ligne ("link" = lien, en anglais) ne faisant pas tout, un site, c'est aussi un bon nombre de disques durs en RAID et si possible suffisamment rapides pour ne pas ralentir le site. Si les petits sites peuvent se contenter de 200 Go d'espace, les plus gros se promènent avec leurs 1, 2, 3+ To de fichiers pirates (1 To = 1000 Go). Oui, ça en fait des disques durs ! Et ça fait aussi cher pour monter un site, c'est pourquoi les sites font souvent appel à de généreux contributeurs (par exemple les gens qui sont doués pour récupérer les disques durs tombés du camion), qui en échange de dons (matériel, $$$) se voient offrir des privilèges comme l'accès illimité au site, un pin's Haribo ou la visite de policiers à une heure indue.
Pour vous donner une vue globale, le circuit d'une release Warez ressemble à peu près au schéma suivant.

Quelques définitions pour les nouveaux venus dans le monde du Warez :
- FXP = File eXchange Protocol = action de transférer des données d'un site FTP à un autre, sans que les données passent par l'ordinateur de la personne qui contrôle le transfert.



SCENE : LE SITEOP

- "pre" = action de rendre publique une release sur un site.
- "trader" = "courier" = personne qui transfère les releases entre les sites FTP, par FXP. Une telle personne a un accès privé à un certain nombre de sites.
- "lamer" = "gros naze" = terme péjoratif utilisé par certains membres de la scène pour désigner ceux qui n'ont pas accès aux meilleures sources de Warez : ce sont tous ceux qui téléchargent sur IRC, les réseaux P2P, les newsgroups, les boards FXP, etc... évidemment, les lamers en question ne se considèrent pas comme tels, il s'agit juste d'une simplification, inutile de nous insulter parce qu'on vous a traité de lamer :) C'était juste pour distinguer les différentes catégories d'utilisateurs.
- je n'ai indiqué les sites web que pour vous rappeler que dans 110 % des cas, il s'agit de sites pourris n'ayant rien à proposer en téléchargement, si ce n'est notre ami Gator l'alligator ou autres AnnaKournikova_naked.exe.

LE SITEOP

Un site, c'est donc une machinerie assez lourde. Un site sérieux se devant d'être en ligne 24h/24, 7j/7, il faut des gens pour s'en occuper au quotidien. C'est là qu'interviennent les siteops. Ils sont en effet plusieurs par site, à gérer diverses tâches comme l'attribution des comptes, les réponses à toutes les questions des utilisateurs, la surveillance de l'activité du site et de ses membres, les problèmes imprévus (pannes matérielles, problèmes de connexion, etc...) et j'en passe.

Commençons par la question des comptes. Evidemment, n'importe qui (au hasard, vous qui lisez cet article) ne peut pas aller voir un siteop (en supposant que vous sachiez où en trouver), lui demander un accès au site et voilà, c'est dans la poche ! Non non, c'est un peu plus compliqué. Sauf si vous êtes un bon ami du siteop en question, que vous le connaissez depuis la maternelle et que vous lui léchez les bottes depuis 10 ans, alors en effet, vous avez une chance. Sachant que chaque utilisateur est identifié par le groupe auquel il appartient, dans ce cas-là, vous ferez sans doute partie du groupe "Friends".

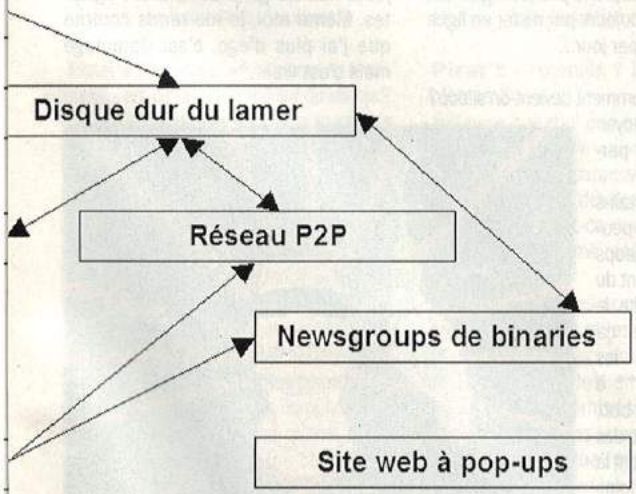
Sinon, vous pouvez être membre d'un groupe "affilié" au site (un "affil"). Un affil est un groupe qui "pre" ses releases sur le site (voir schéma). Le choix des affils est très important pour un site. Avoir des affils prestigieux (comme DEViANCE pour les jeux, ViTE ou CENTROPY pour les films, etc) ajoute beaucoup à la renommée du site. Ce sont les siteops qui choisissent les affils. Evidemment, il s'agit d'un accord mutuel : réciproquement, les affils cherchent à être sur les meilleurs sites possible (les plus sécurisés, les plus rapides, les plus gros, les plus stables, ceux qui ont d'autres bons affils, et dont l'adresse IP n'est pas en .gouv). Un groupe renommé va se voir offrir énormément de sites et devra faire un choix, car il est difficile d'uploader la même release sur 150 sites à la fois. Les groupes moins connus devront eux se contenter de sites plus petits, en espérant monter dans la hiérarchie plus tard. De même, les gros groupes ont de plus grandes exigences : plus de slots (nombre de membres du groupe autorisés sur le site), dont plus de leechs. Un compte leech s'oppose au compte traditionnel soumis à un ratio (on peut télécharger 1 Mo seulement si on a déjà uploadé x Mo auparavant - typiquement, x = 1/3) : un compte leech a un ratio de 0, c'est-à-dire qu'on peut télécharger à volonté. Le siteop doit donc essayer de satisfaire les exigences du groupe tout en restant équitable avec les autres groupes, et en évitant de pénaliser le site en étant trop généreux.

Enfin, la seconde grande catégorie d'utilisateurs, ce sont les traders (ou couriers). Ce sont des gens dont la seule fonction est de prendre une release sur un site pour l'uploader (par FXP) sur un autre site, et ainsi la répandre. Comme nous reviendrons sans doute là-dessus dans un prochain numéro, je ne vais pas m'étendre. Sachez qu'au total, un nombre "moyen" de membres sur un (gros) site pas trop privé tourne autour de 100-200 personnes. Ca fait du monde à surveiller pour les siteops, qui vont notamment mettre à la porte les traders trop fainéants (ceux qui n'uploadent pas un minimum) ou qui violent constamment les règles du site.

En parlant de règles justement, l'une des tâches du siteop c'est également de pondre un ensemble de règles qui déterminent ce qu'il est possible de faire sur le site, notamment ce qu'on a le droit d'uploader. Par exemple ces règles peuvent être :

---+++ GENERAL +++---
- If you talk about this site outside of channel-[deluser]
- If you complain to the siteops--[deluser]
- No echoing of the sitebot----[deluser]
- Upload must be completed within 2h----------[2x]

---+++ GAMES RULES +++---
- Only PC games----------[3x]
- Release must be within 6 months from retail----------[2x]



ÇA HACKE SÉVÈRE À MEXICO !

Incroyable mais vrai : un pirate de génie est parvenu à piller des dizaines de comptes d'une des plus grandes banques du Mexique, détournant ainsi par Internet quelques 1,5 millions de pesos (soit environ 130 000 euros) ! La banque, la Banamex-Citibank, était située dans l'Etat de Nuevo Leon, au nord du pays. Le pirate a eu la bonne idée de repérer les comptes de clients qui n'avaient pas de mouvements réguliers. Il court toujours, à la fureur des banquiers et des clients lésés. Eh, gringo, si tu nous lis, fais gaffe à tes fesses !

L'UNION EUROPÉENNE SUR LE PIED DE GUERRE

Afin de lutter contre les attaques potentielles de pirates, l'Union Européenne a décidé récemment d'harmoniser les lois anti-piratage courantes dans les pays européens. D'ici le 31 décembre 2003, ils devront se mettre d'accord, sous peine de sanctions. Jusqu'ici, il est vrai qu'aucun plan d'envergure n'avait été mis à l'œuvre contre le cyber crime, qui profitait des lacunes juridictionnelles ou des législations libérales pour prospérer en toute impunité. C'est en tout cas un sévère coup de vis qui s'annonce.

IL N'Y A PAS D'ÂGE POUR PIRATER

On a peut-être trouvé le hacker le plus jeune de l'Histoire : il s'agit d'un gamin de 11 ans, américain of course. Le petit malin, qui réside en Floride, avait tenté de modifier ses notes de fin de trimestre. La sanction a été sévère : le principal du collège a exigé que le petit soit renvoyé définitivement. En plus de cela, il a dû passer une journée en prison ! La " tolérance zéro " est bien à l'œuvre aux Etats-Unis... Après tout, n'a-t-il pas commis une simple bêtise comme tout autre enfant du même âge ? Ou peut-être avait-il lu Pirat'z ?

WAREZ

LINUX S'APPROPRIE LA XBOX

On vous rapportait dans le numéro précédent que le "Xbox Linux Project", groupe dédié au développement de distributions Linux pour Xbox, avait cherché l'appui de Microsoft pour que soit autorisée l'exécution de Linux sans modchip (ce qui était jusqu'alors impossible). Depuis, ils ont également dénoncé Microsoft à la Commission Européenne (l'accusant de profiter abusivement de leur position monopolistique). Mais finalement, il se pourrait bien qu'on puisse se passer de l'accord de Billou! En effet, quelqu'un est parvenu à cet "exploit", en exploitant justement un buffer overflow dans le jeu "007 Agent Under Fire", par l'intermédiaire d'une sauvegarde modifiée. Le fichier est dispo sur la page du projet (www.xbox-linux.com - mais attention, il s'agit d'un fichier .txt encodé, que vous pouvez par exemple décoder avec WinRar pour obtenir le .zip original). Evidemment, vous devez aussi avoir le jeu 007, ainsi que le matériel nécessaire pour charger la sauvegarde modifiée depuis votre Xbox. Et là, comme par magie, vous pouvez lancer Linux! Chapeau.

ALPAGUÉ

Il existe sur le net de nombreux sites fonctionnant comme annuaires de liens vers le réseau eDonkey. Ces sites visent à faciliter l'accès aux ressources du réseau, et se protègent derrière le fait que les fichiers ne sont pas hébergés sur le site. Pourtant, le Edonkey-divx.com a dû fermer boutique suite à une action de l'ALPA (Association de Lutte conte la Piraterie Audiovisuelle), qui n'appréciait guère d'y voir des milliers de films en téléchargement. On recherche toujours le webmaster, vu pour la dernière fois à Irkoutsk, en Sibérie.

Il ne s'agit évidemment que d'un petit extrait, il peut y avoir des dizaines de règles. "deluser" signifie suppression du compte. "2x" signifie que ce qui a été uploadé va être "nuké" d'un facteur 2, c'est-à-dire que la personne qui l'a uploadé va perdre en crédits 2 fois la quantité uploadée (les crédits sont le nombre de Mo qu'on peut télécharger, et on gagne des crédits en uploadant). Par exemple, si j'ai 2 Go de crédits et que j'uploade un jeu pour Mac de 600 Mo sur ce site, je me retrouve avec seulement 200 Mo (au lieu des 3,8 Go que j'aurais atteints si la release n'avait pas été nukée). Enfin, sachez que si les siteops édictent les règles, ce sont le plus souvent les nukers qui les font appliquer (c'est leur job sur le site).

Terminons avec un petit point sur les mesures de sécurité du site. Evidemment, un site ne doit pas être public, visible aux yeux de tous (et du FBI notamment). Le serveur FTP tourne généralement sur un port non conventionnel (certainement pas le port 21 en tout cas), et n'est pas accédé directement par les utilisateurs : un site utilise des bouncers (ou BNC) sur lesquels on peut se connecter. Le bouncer effectue l'authentification par IP et ident (un service d'authentification venant du monde Unix, pour avoir une ident vous devez avoir un serveur ident tournant sur votre port 113). Si (et seulement) si l'authentification est réussie, vous êtes redirigé ("bouncé") automatiquement sur le serveur FTP. Ainsi, vous n'avez jamais l'adresse IP du serveur (bien sûr, vous pouvez la trouver, mais l'utilisateur "moyen" n'en a pas besoin). Et si quelqu'un tombe sur vos infos de connexion (comme l'IP du bouncer), il ne pourra pas avoir accès au serveur (pour le hacker par exemple) puisqu'il ne pourra pas passer la barrière du bouncer. Comme autres mesures de sécurité logicielles, certains sites interdisent les transferts vers certains ranges d'IP jugés "dangereux" (sites universitaires, bureau de G.W Bush). Il y a également bien sûr des mesures de sécurité locales pour éviter que le site soit découvert (il est rare que toute la compagnie trempe dans le trafic de logiciels pirates, c'est toujours le responsable réseau le coupable (mais non bien sûr, c'est bien connu que le responsable réseau n'y connaît rien en informatique, le coupable est donc le fils du directeur qui a installé une backdoor sur la machine de son père et contrôle à distance tout le réseau de l'entreprise)). Enfin bref, la grosse bécane qu'est le site doit éviter d'être trop voyante, et bien sûr ne pas être accessible à n'importe qui. Les siteops doivent aussi être au courant de tout cet aspect, souvent à distance, par l'intermédiaire de personnes de confiance.

UN SITEOP, UN VRAI !

Et pour compléter cet article, nous n'avons rien trouvé de moins que d'interviewer directement un siteop ! Croyez-moi, ce n'est pas une tâche des plus faciles, car il s'agit d'une personne sérieusement impliquée dans la Scène, à un niveau assez élevé : on ne fait pas les choses à moitié à Pirat'z ! L'interview a eu lieu sur IRC - le lieu de rencontre par excellence de tous les groupes pirates. Evidemment, le siteop ne souhaitait pas que nous communiquions des informations personnelles le concernant, nous ne vous révélerons donc pas son nick, ni sa nationalité. De toute manière, son nick était certainement changé pour l'occasion, et son IP était masquée, s'agissant d'un réseau IRC privé anonyme... Enfin, finis les blabla, laissons la parole à un vrai siteop :

Pirat'z : Bonjour.
Siteop : Salut.

Pirat'z : Peux-tu nous résumer en une phrase le rôle du siteop ?
Siteop : Mon rôle est de coordonner les membres et les affils pour avoir un bon site sur lequel ils puissent se sentir en sécurité.

Pirat'z : Et quelles sont les tâches quotidiennes d'un siteop ?
Siteop : Héhé, et bien, en gros j'autorise les nouvelles IPs d'au moins 5 personnes par jour, et à part ça, pas grand-chose.

Pirat'z : Ce n'est donc pas un travail trop difficile on dirait !
Siteop : En fait, il y a bien sûr parfois des problèmes à régler avec les affils, mais je ne considère pas cela comme une tâche quotidienne. Finalement, si on y réfléchit, ça ne prend pas si longtemps, mais on finit toujours par rester en ligne au moins 5 h par jour...

Pirat'z : Et comment devient-on siteop? Y a-t-il un moyen spécifique d'y parvenir ?
Siteop : Certains pensent qu'ils peuvent devenir siteops juste en donnant du matériel à un site. Je suppose que ça marche pour les sites de m**** à 10 Mbits/s sur bbb, mais si on parle des gros sites qui sont là depuis au moins 2,3 ans, donner du matériel ne t'apportera rien sinon un beau doigt !

Pirat'z : Et toi ? Peux-tu nous dire comment tu es devenu siteop d'un de ces "gros sites" ?
Siteop : Le site que je gère, je l'ai démarré il y a trois ans moi-même avec quelques amis que je connaissais depuis quelques années déjà, donc nous n'avons jamais engagé quiconque dans le staff pour avoir donné du matos ou quoi que ce soit d'autre. C'est juste que je n'ai pas confiance dans les gens qui essaient d'acheter leur ticket d'entrée de cette façon. N'importe qui peut acheter 40 disques de 200 Go et en faire un gros site avec un lien rapide, mais ce n'est pas ce qui fait le site : ce sont les personnes derrière le site qui importent vraiment.

Pirat'z : D'accord. Et un siteop a-t-il systématiquement un accès physique au serveur ? Ou y a-t-il des sites avec aucun siteop sur place ?
Siteop : Les siteops n'ont presque jamais un accès local, puisque les gros sites sont situés dans des endroits plus sécurisés qu'une bête maison (comme c'est le cas pour les sites suédois sur bbb). Dans le cas des gros sites, il y a donc généralement des gens qu'on appelle des "admins", et ce sont eux qui sont sur place.

Pirat'z : Et ceux-ci ne sont donc pas nécessairement impliqués dans la Scène ?
Siteop : Non. Très peu d'entre eux le sont.

Pirat'z : Pour revenir à ce que tu disais auparavant... qu'est-ce qui fait un bon site ? La connexion ? Le matériel ? Les affils ? Les siteops ? Les traders ?
Siteop : Je dirais qu'on ne peut pas avoir un bon site sans de bons siteops pour commencer, bien sûr !
Mais on dirait que de plus en plus aujourd'hui, les gens deviennent égoïstes. Même moi, je me rends compte que j'ai plus d'ego, c'est dommage mais c'est vrai...

Pirat'z : Egoïstes ? Dans quel sens ?
Siteop : Et bien, ils ne pensent qu'à eux-mêmes et au site, ils considèrent les traders comme des idiots qui peuvent être remplacés quand on veut. Pour eux, ce sont des points, pas des êtres humains. Si tu as quelques mauvais points sur ton site, tu t'en débarrasses et tu les remplaces par d'autres points qui font mieux leur boulot.

Pirat'z : A ce sujet, ça me rappelle avoir déjà entendu parler de techniques pour auto-dupliquer le contenu de sites entre eux, ce qui permettrait de se débarrasser de ces "idiots" de traders... tu penses que ce serait une bonne chose ?
Siteop : Hmm... si par exemple je créais un site US de 3 To avec un lien à 1 Gbit/s, je n'aurais aucun "vrai" affil ou trader dessus, tout simplement parce que c'est trop beau pour être vrai. Et je pourrais vouloir utiliser une telle technique. Mais de toute façon ça ne marche que pour les Etats-Unis [NB: de tels sites existent plus couramment en Europe]. Donc pour l'instant, pour moi, c'est non, ça n'apporte rien de vraiment intéressant.
Cela dit, je connais quelques sites qui le font entre leurs propres sites. Je m'explique : supposons que tu as un beau gros site, grâce à tous les fournisseurs en matos. Où mets-tu tous les leechers [NB: ceux ayant un compte leech] qui ont donné le matériel ? Certainement pas sur le vrai site, héhé, tu mets à côté un petit site pourri de 10 Mbits/s avec un script pour auto-dupliquer le contenu du vrai site, et *pouf*, tout le monde est content ! Même si ça veut dire qu'il faut 2 bécanes, la deuxième n'a pas besoin d'être plus grosse que 200 Go puisque les leechers téléchargent les nouveautés et n'ont rien à faire des grosses archives [NB: un site de 3 To va contenir énormément de vieilles releases, qui forment les "archives"]

Pirat'z : Revenons au problème de la sécurité... est-ce un souci majeur du siteop ?
Siteop : Oui bien sûr, garder le site sûr est, au moins pour moi, l'objectif principal.

Pirat'z : As-tu déjà failli être attrapé ?
Siteop : Nous nous sommes déjà fait prendre une fois. Mais pour ce lien-ci qu'on utilisait à l'époque, nous avions 15 admins sur place qui nous connaissaient et travaillaient pour abuse@isp [NB: ceci sous-entend que le site était hébergé chez un fournisseur d'accès, et que ceux qui ont reçu la plainte étaient donc complices]. Ils ont déménagé la machine quand ils ont reçu le mail de la MPAA (ou du BSA, ou des policiers, je ne sais plus trop). C'est ça un gros site, il y a moins de problèmes de sécurité qu'avec les sites hébergés dans une chambre d'université.
Pirat'z : Donc dans ce cas-là, le site avait en fait déjà disparu avant que les flics aient pu le saisir ?
Siteop : Oui, bien longtemps avant. Nous avions aussi effacé toutes les données au cas où ils seraient parvenus jusqu'à lui, mais comme nous l'avions déplacé vers une autre ville, c'était peu probable.

Pirat'z : Mais alors pourquoi être siteop, avec tous les risques que ça comporte ?
Siteop : Honnêtement, je n'en sais rien... Je fais ça depuis 6 ans et je n'envisage pas d'arrêter, je suppose que c'est un passe-temps comme un autre. J'aime l'idée de pouvoir essayer un logiciel avant de l'acheter, de la même façon qu'on n'achète pas une voiture sans l'avoir conduite auparavant.

Pirat'z : Est-ce que tu achètes vraiment des logiciels ?
Siteop : Oui, bien sûr ! Les deux derniers jeux que j'ai achetés, c'est Command and Conquers : Generals, et Battlefield 1942.

Pirat'z : Et ce sont de bons jeux ?
Siteop : Oui, excellents ! J'y joue sur le net avec des amis.
Je pense que je n'irais jamais regarder les jeux dans une boutique de jeux vidéo. Par contre, quand tu peux les télécharger et les tester gratuitement... Moi, quand j'aime un jeu, je l'achète. Et j'ai de nombreux amis dans la Scène qui eux aussi achètent leurs logiciels.

Pirat'z : Pour finir avec la sécurité... ne penses-tu pas que les sites devraient utiliser un protocole de transmission crypté ?
Siteop : Si, bien sûr. Et quand ça fonctionnera comme ça le devrait, c'est-à-dire sans aucun problème, alors je l'installerai sur mon site.

Pirat'z : Pourquoi ? Il y a des problèmes ?
Siteop : Je n'ai pas encore entendu parler d'une version vraiment fiable pour l'instant, donc je suppose que c'est encore en cours de développement. Mais après tout, qu'est-ce que j'en sais... je devrais peut-être me renseigner.

Pirat'z : Quelles sont les relations entre les groupes et les siteops ? S'agit-il de personnes complètement différentes ? Ou les siteops sont-ils souvent aussi membres de groupes ?
Siteop : Certains groupes ne parlent à leurs siteops que lorsqu'ils ont besoin d'eux. D'autres les traitent comme membres à part entière de leur groupe, ça dépend vraiment de comment les gens se connaissent, avant et pendant l'affiliation.

Pirat'z : La Scène est-elle un petit monde assez fermé, où tout le monde connaît tout le monde ?
Siteop : Je suppose que beaucoup pensent que c'est un monde fermé. Mais je rencontre de nouvelles personnes tous les jours, bien que je change de nick de temps en temps pour éviter que tout le monde se mette à me harasser. Je ne veux pas vraiment connaître plus de gens, je sais que ceux que je connais ne posent pas de danger, et j'ai suffisamment de connexions pour faire tout ce que je désire. Je ne vois donc pas de raison pour m'impliquer avec plus de monde, et j 'essaie de garder un profil bas.

Pirat'z : Y a-t-il une compétition importante entre les sites ? Entre les siteops ?
Siteop : Et bien, entre les siteops, certains siteops en détestent d'autres à cause de leur site, j'en ai moi-même fait l'expérience... Et entre les sites, bien sûr que c'est la compétition, il faut toujours être le plus rapide, ou avoir les meilleurs affils... Et moins il comporte de membres, meilleur est le site. C'est sûr qu'on peut ajouter 500 personnes dessus, mais quel vrai trader va s'intéresser à un site tellement "public" ? Un bon site maintient une sélection sévère, contrairement aux bbb 10 Mbits où n'importe qui peut obtenir un compte.

Pirat'z : Et toi, tu as beaucoup de gens qui viennent de demander un compte sur ton site ?
Siteop : Je ne fais pas de publicité pour mon site, et je n'y invite que les traders qui m'intéressent personnellement, donc non, il n'y en a pas beaucoup qui viennent. Mais si quelqu'un me demande, je leur pose toujours la question "eh, qui t'a dit de me contacter ?", et si j'arrive à le découvrir, je supprime le compte de celui qui lui avait dit. Je n'apprécie pas les gens qui parlent trop. Ils peuvent bien parler, mais ils ne seront sur aucun de mes sites, avec leur grande gueule.

Pirat'z : Tu as beaucoup de sites, au fait ?
Siteop : Quelques-un, oui, mais tous très privés.

Pirat'z : Une dernière question : penses-tu que la Scène va continuer de fonctionner comme maintenant ? Ou vois-tu des changements arriver ?
Siteop : Déjà, je vois plus de gens égoïstes... Les sites seront de plus en plus privés, et enfin j'espère que le problème de la sécurité des transferts de fichiers va finir par être résolu.

Pirat'z : Et bien, merci beaucoup !
Siteop : Y'a pas d'quoi :)

LE FBI REMET ÇA

Certains d'entre vous se souviennent peut-être du 11 décembre 2001, lorsqu'une vaste opération du FBI, en coordination avec d'autres forces policières dans le monde, avait abouti à l'arrestation de nombreux membres de groupes pirates. Le groupe DrinkOrDie, principale victime dans l'affaire, avait notamment été démantelé. Et bien, ils nous ont remis ça, bien qu'en version "light": si certains groupes et sites ont fait profil bas pendant quelques jours, il n'y a pas eu une quasi-totale interruption de l'activité de la Scène comme il y a 1 an et demi. Bon, que s'est-il passé cette fois-ci? Au moins 4 sites américains et suédois ont été saisis par le FBI et leurs amis, ainsi que certaines des personnes gravitant autour. Ceux-ci risquent gros, puisqu'on se souvient que certains membres de DrinkOrDie sont en prison, et encore pour un petit bout de temps... Il est difficile de savoir exactement qui a été visé, les rumeurs allant bon train. Une petite collection de rumeurs non vérifiées se trouve d'ailleurs sur: http://193.220.101.72/info/

CRASHER IE EN 1 LEÇON

Une vulnérabilité dans Windows XP et Internet Explorer depuis la version 4.0 peut être exploitée pour causer une attaque DoS. Il est ainsi très facile de faire planter IE avec une minuscule page HTML d'une seule ligne. Ok ça ne veut rien dire, on peut faire beaucoup de choses en HTML sur une seule ligne, mais je vous donne un exemple de code: <html> <form> <input type crash> </form> </html>. Ecrivez ça dans un fichier .html, ouvrez-le avec IE... et *crash*! A moins que MS ait corrigé la faille depuis, mais j'ai comme un doute...

COURRIER DES LECTEURS

A tous les lecteurs qui souhaitent nous écrire avec leurs petits doigts boudinés, l'adresse est toujours piratgamez@yahoo.fr, et nous répondrons avec plaisir à tous ceux qui veulent des adresses de sites illégaux, ou savoir comment pirater le mail de leur meilleur ami, ou le code d'un virus mortel pour faire une bonne blague à leur papa... par "désolé, ce n'est pas la bonne adresse !". Par contre, pour nous féliciter, nous engueuler, nous confier vos chagrins d'amour et les dernières failles que vous avez découvertes, pas de problème !

ÇA SAQUE DUR SUR LES CAMPUS AMÉRICAINS !

L'industrie de la musique a encore frappé aux Etats-Unis : sa colère s'est tournée contre 4 étudiants, accusés d'avoir diffusé des millions de chansons sur leurs campus respectifs, grâce à leurs réseaux Internet locaux. Au menu, que des gros poissons : Springsteen, U2, Eminem ou encore Madonna. Tant d'artistes qui s'estiment lésés par les échanges de fichiers qui émanaient des campus. Aujourd'hui, les accusés risquent de payer jusqu'à 150 000 $ par titre diffusé. De quoi avoir follement envie de ressortir ses vieux 33 tours...

LE HOAX QUI N'EN FINISSAIT JAMAIS

Cela fait maintenant plusieurs années que le même hoax tourne sur Internet : le message selon lequel la maison Veuve Clicquot offrirait une caisse de six bouteilles de champagne aux internautes qui font suivre le message à dix autres personnes n'arrête pas de se propager de boîte en boîte. Le canular le plus nul et le moins vraisemblable de la Terre continue donc de sévir. À tel point que la vénérable maison Clicquot s'est fendue fin mars 2003 d'un communiqué officiel précisant qu'elle n'était pas l'auteur de cette offre. Sans blague ?

ÉTEIGNEZ VOS PORTABLES !

Rien à faire : le citoyen étant incapable de se discipliner lui-même, la municipalité de New York a décidé de sévir. Depuis le dimanche 13 avril, tout gêneur qui voudra utiliser son téléphone portable dans un lieu public comme les théâtres, les bibliothèques, les musées, les cinémas ou les salles de concert se verra infliger une belle amende de 50 $ (environ autant d'euros) ! De quoi convaincre rapidement les plus récalcitrants de laisser leurs portables au vestiaire... Vivement qu'une telle mesure arrive en France !

Tout d'abord merci pour la qualité du mag. Dans le numéro 1 de Pirat'z vous parlez de PGPdisk pour crypter les infos d'un disque dur et ainsi les protéger. Personnellement je suis un peu plus tordu, et je voudrais votre avis. Je fonctionne sous XP (je sais personne n'est parfait ;) et j'utilise le tout petit utilitaire nommé Hide Folders XP. Il permet de cacher totalement un dossier de sorte qu'il n'apparaît plus nulle part. J'ai supprimé Hide Folders XP de la liste des programmes installés, et j'ai renommé le fichier exécutable avant de le cacher dans le dossier System32 (ce qui me permet de le lancer directement dans la commande Exécuter du menu Démarrer). Evidemment la liste des commandes tapées s'efface à chaque reboot.
En clair personne ne sait que j'ai installé ce prog et personne ne peut voir les dossiers que j'ai protégés.

SCHEDADEX

C'est pas mal, et ça suffit sans doute, à un petit détail près : les informations sont toujours en clair sur le HD, donc peuvent être récupérées avec des logiciels spéciaux. Voire même des logiciels pas spéciaux du tout, puisque ça ne marche que sous Windows : si on boote sous Dos avec une disquette (et qu'on utilise par exemple NTFSDos pour lire la partition XP), on voit parfaitement les répertoires cachés. C'est donc bien tant que personne ne se doute qu'il y a quelque chose de caché, mais dans le cas contraire, tes fichiers confidentiels pourront facilement être dévoilés.

J'ai découvert une nouvelle petite faille à la c, mais les petits riens font grandir le monde (je ne sais pas qui a dit ça mais c'est bien). Il est assez difficile de pirater une boite AOL, pourtant, j'ai découvert une astuce théorique (je ne l'ai pas encore essayée mais je crois que ça marche).**

Chaque compte a une page perso et le pass FTP est le pass de connexion AOL. Donc, si on fait une attaque brute force, on est censé découvrir le pass AOL !

CYBER-FLAT

En effet, cette faille pourrait être en théorie utilisable si le mot de passe est choisi par l'utilisateur. Mais es-tu sûr que c'est bien le cas sur AOL ? C'est à voir (je ne peux pas vérifier moi-même, je ne connais personne sur AOL, je choisis bien mes amis, moi !). Dans le cas contraire, ça serait bien trop lent de faire une telle attaque par le réseau, on aurait bien peu de chances de découvrir le mot de passe.

SALUT,
SAIS-TU QUE DANS GHOST MAIL, IL Y A UN CHEVAL DE TROIE ? JE L'AI TÉLÉCHARGÉ, JE M'EN SERVAIS POUR VOULOIR FAIRE DE BONNES BLAGUES À MA FAMILLE, ÇA MARCHAIT JAMAIS ! C'ÉTAIT LE SERVEUR QUI ÉTAIT INACCESSIBLE, J'EN AVAIS MARRE J'AI QUITTÉ CE * DE LOGICIEL. LE LENDEMAIN, J'AI INSTALLÉ ANTI-TROJAN V.5.5 SHAREWARE, J'EXÉCUTE LA RECHERCHE PAR HASARD, ET IL TROUVE BON NOMBRE DE PORTS OUVERTS, PLUS QUE LA NORMALE, ET APRÈS DÉTECTE LE CHEVAL DE TROIE DANS GHOST MAIL.EXE, DANS LE RÉPERTOIRE OÙ IL ÉTAIT, ET ÇA NE POUVAIT ÊTRE QUE CELUI-LÀ. J'EN AI PARLÉ À D'AUTRES GARS, ILS M'ONT DIT QUE OUI, ILS AVAIENT UN CHEVAL DE TROIE DANS LEUR GHOST MAIL.EXE, MAIS QUE C'ÉTAIT UN ANCIEN CHEVAL DE TROIE.**

MAX

Bon, on arrête la parano, il n'y a pas de Trojan dans Ghost Mail ! Le programme est en effet reconnu comme cheval de Troie par certains anti-virus, mais pas parce qu'il ouvre des ports permettant une attaque d'un hacker (si tu avais plus de ports ouverts que d'habitude, tu devrais donc t'inquiéter !). C'est surtout parce que quelqu'un pourrait prendre le contrôle de votre machine (tout à fait indépendamment de Ghost Mail), puis utiliser Ghost Mail pour envoyer des mails anonymes, qui vous seraient attribués. Les anti-virus, considérant que l'utilisateur moyen n'utilise pas Ghost Mail, préfèrent te prévenir de sa présence au cas où ce ne serait pas toi qui l'utiliserais !

Bonjour,
Je voudrais savoir comment faire pour mettre des jeux PS2 avec l'extension .bin en NTSC ou en PAL et vice-versa avant la gravure. Exemple : j'ai un jeu PS2 que je passe en *.bin, comment savoir si le jeu à ce moment est en NTSC ou PAL ? Et comment le convertir dans l'autre format ?

TI TITI

Il te faut un patch NTSC -> PAL (convertit un .bin NTSC vers PAL), PAL->NTSC (l'inverse) ou un patch NTSC/PAL selector (permet de choisir !) pour la version de ton jeu. C'est facile, si tu as acheté ton jeu pour une console européenne, le .bin que tu obtiens en en faisant l'image est en PAL, sinon ça sera du NTSC. Pour les patches, tu peux en trouver plein sur :
http://www.megagames.com/ps2/ps2_patches.shtml
http://spiv.de/ps2
http://www.adr-uk.com/site/download.php?op=viewdownload&cid=5

LE 1ER MAGAZINE DE LA PERFORMANCE INFORMATIQUE

NOTRE CONCOURS : TOUS LES RÉSULTATS

n°4

JUIN- JUILLET 2003

OVERCLOCKING News

LE 1ER JOURNAL DE LA PERFORMANCE INFORMATIQUE

FOUDROYANTE !
GEFORCE FX 5900 ULTRA
C'EST LA CARTE VIDÉO
LA PLUS RAPIDE AU MONDE

BANC D'ESSAI

VENTIRAD
VANTEC
AEROFLOW
VP4-C7040

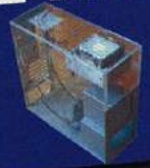
ALIMENTATION SURPUISSANTE
TOPOWER 470W

3,90€ BIMESTRIEL

L 19354 - 4 - F: 3,90 € RD

NOS PERFORMANCES
NOUS AVONS OVERCLOCKÉ DEUX PROCESSEURS :
UN ATHLON XP 1700+ À 2500 MHZ
ET UN CELERON 2 GHZ À 2,8 GHZ

LE MODE D'EMPLOI DU WATERCOOLING



Bien choisir ses composants
Comment les intégrer dans une tour
Un boîtier Crist0 à construire soi-même

DÉJA EN KIOSQUE

Le Best-of du net pirat'Z

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

HACKING et SECURITÉ INFORMATIQUE

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

SAUVEGARDE et DEVELOPPEMENT

-Génériques

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

-Copie (gravure, modchips, ...)

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

-Spécifiques à certaines machines

Programmer's tools. Tous les outils du programmeur Windows pour le reverse-engeneering : protools.cjb.net
Xbox Scene. Toute l'actualité de l'underground Xbox : www.xbox-scene.com
Xbox-Linux. Installez Linux sur votre Xbox : xbox-linux.sourceforge.net
Spiv's no-mod central. Des tas de patches pour PS2 : www.nomod-central.com
PS2Ownz. Des infos et des forums bien remplis sur la PS2 : www.ps2ownz.com
Backup-Source. La sauvegarde sur PS2 et Xbox : www.backup-source.com
Guide copie Dreamcast. Et en français en plus : membres.lycos.fr/raptor83/dreamcast/copie.htm
Réalisation d'un câble DC->PC : www.ifrance.com/hack128/burn_o.htm

TELECHARGEMENT et ACTU PIRATE

-Web

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

-Peer-to-Peer

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

-FTP, 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.abandonware-ring.com
Classic Trash. Un des sites d'Abandonware les plus respectés : www.classic-trash.com
Home of the Underdogs. Une référence de l'Abandonware que vous ne pouvez pas manquer : www.the-underdogs.org
Oldiesfr.com. Un site moins fourni, mais en français : www.oldiesfr.com
VDMSound. Pour un son parfait dans les vieux jeux : ntvdm.cjb.net

-Emulation

Zophar's Domain. L'ancêtre est toujours là : www.zophar.net
Emu Unlim. Site très complet dédié à l'émulation : www.emuunlim.com
Linux Emu. L'actualité de l'émulation sous Linux: linuxemu.retrofaction.com
NGEmu. Surtout utile pour PSX / N64 / DC / GBA / Saturn : www.ngemu.com
Emu-France. Un site français très complet sur toute l'actualité de l'émlation : www.emu-france.com
Toudy. Un site bien sympa en français : www.toudy.com
Emulation64. Toute l'émulation N64 en français : www.emulation64.net
Pdroms. Des tas de roms freeware : www.pdroms.de (les downloads devraient être réactivés le 1er juin)

JEU ONLINE

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

CHEATS

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