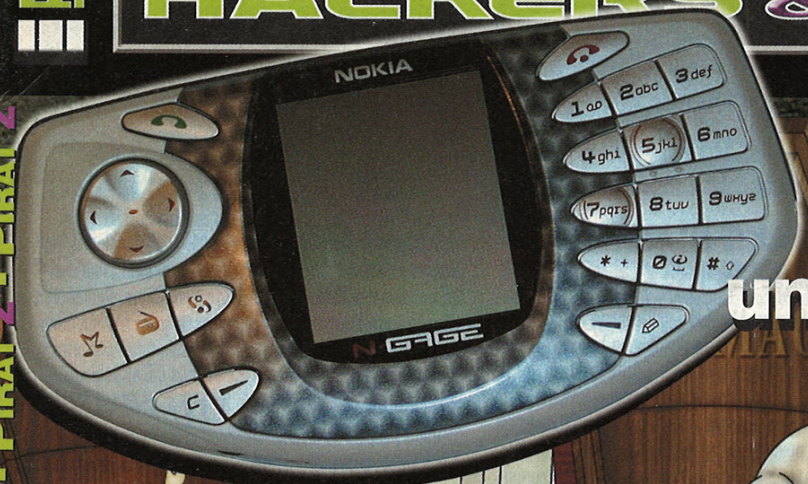
N°5 DÉCEMBRE-JANVIER - THE ORIGINAL HACKER SYNDIKATE

PIRAT'Z

HACKERS & GAMERS



Gagnez une N-GAGE NOKIA FACILE !

Notre concours p 25

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

1,5 €

LECHATKITU

NICKEZ LES SPAMMERS • pirater les users
eMule • GAME CUBE Hacked
BITTORRENT le P2P ultra rapide • MATRIX
PLOOF! • OLD SCHOOL : back to 80's

TOUT CRACKER : JEUX, LOGICIELS, MOTS DE PASSE

EDITO

Vous auriez pu nous reprocher de ne pas parler assez des téléphones portables dans Pirat'z. Pour couper court à toutes les critiques dans ce sens, nous avons décidé de vous en offrir un, et pas des moindre puisqu'il s'agit du N-Gage de Nokia. Vous savez, ce n'est pas grand chose, vu que nous en recevons des tonnes toutes les semaines. Si, si, les opérateurs télécom veulent nous faire taire les faiblesses que nous découvrons régulièrement sur leurs réseaux.

Et qu'on ne nous traite pas d'élitistes parce qu'il faut répondre à des questions pour gagner l'appareil. La plus grande difficulté consiste à trouver la page du concours. Nous avions pensé à vous faire écrire un shellcode polymorphique pour SPARC ou à vous faire rédiger un article d'analyse sur la philologie du jargon des hackers pour le prochain numéro. Rien ne vous empêche de relever ces défis. Mais comme vous n'avez sans doute pas que ça à faire, nous avons préféré un questionnaire qui ne vous prendra que quelques minutes – à fouiller dans vos archives de Pirat'z, naturellement. Enfin prezque, vous verrez :-)

Pour le reste des critiques, vous n'avez qu'à vous adresser à Khan, poste restante, Iles Fiji. Le malappris est parti avec la caisse et les numéros de cartes bleues de tous les abonnés. Un matin, nous avons retrouvé un mot sur son bureau vide : " Adieu les amis, et bonne chance. Je pars pour des lieux plus propices à passer ces durs mois de fin d'année. Dites mes plus vifs sentiments aux lecteurs, que je ne les oublierai pas, et que Pirat'z doit continuer quoi qu'il arrive. Mon plus grand regret sera de ne plus pouvoir inventer ces histoires à dormir debout pour remplir l'édito. " Bon, soyons justes, il écrit toujours des articles pour Pirat'z et continue à répondre à vos nombreux courriers, en passant par la backdoor qu'il a placée sur notre compte mail.

DE BAZANDE

PIRAT'Z
HACKERS & GAMERS

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

Rédacteur en chef : de Bazande
Conception Graphique : Weel
Illustrations : Lechatkitu, yok2003, Frid
Imprimé en CE

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

Directeur de Publication : Olivier André

SOMMAIRE

MANDRAKE N'AIME PAS CERTAINS LECTEURS

Mauvaise nouvelle pour Mandrake, qui connaît un petit problème dans la version 9.2 de sa distribution Linux: le kernel, en envoyant une commande FLUSH_CACHE au lecteur CD, risque d'effacer ainsi son firmware sur certains lecteurs de la marque LG Electronics. Du coup, adieu le lecteur CD, qui sera bon à jeter à la poubelle, avec le CD Mandrake si possible. Lorsque vous lirez le mag', le problème sera peut-être corrigé, mais dans le doute vérifiez quand même… Toutes les infos sont sur http://www.mandrakelinux.com/en/lgerrata.php3.

UN JOYSTICK POUR " RESSENTIR " LES OEUVRES D'ART

L'IInstitut de Recherche en Informatique de Toulouse a mis au point un outil informatique permettant aux aveugles de "visualiser ". Il s'agit d'une sorte de joystick " à retour de force " transmettant les formes d'une œuvre d'art affichée sur un écran d'ordinateur. Le principe repose sur une " résistance " dans la main tenant le Joystick censée traduire en sensation les aspects visuels de l'œuvre.

HALF LIFE 2 PREND L'AIR

Half Life 2 est sans aucun doute l'un des jeux les plus attendus par les amateurs de FPS. Valve le développe maintenant depuis 5 ans, et la date de sortie maintes fois repoussée semblait enfin s'être stabilisée vers l'automne 2003… sauf qu'un petit cafouillage a changé les plans: le code source du jeu a été volé. Enfin, pas volé, mais copié et distribué sur le net. Les hackers auraient piraté le réseau de la compagnie, en utilisant à l'origine une faille dans Outlook, puis en installant des keyloggers afin de récupérer les mots de passe et ainsi avoir accès à tout le réseau. Un scénario assez abracadabrant mais confirmé par Valve, qui en a profité pour insinuer que ça risquait d'avoir des conséquences sur le développement du jeu (comprenez qu'il sera encore retardé - probablement jusqu'en avril 2004). Si la totalité du code ne serait pas dans la nature, on peut trouver sur le net une version compilée prévue pour jouer à Half Life et Counter Strike avec le moteur du 2ème. Remarquez, c'est pas si mal, ça permettra aux fans de jouer à ça en attendant!

PROTECTIONS VIRTUELLES

Certains adeptes du reverse-engineering (comprenez, des crackers) auraient dévoilé que Macrovision faisait de gros efforts pour améliorer ses protections de jeux. Rappelons que Macrovision est notamment l'auteur de la protection SafeDisc, célèbre pour protéger inutilement des milliers de jeux crackés qu'on peut trouver sur le net. La nouveauté serait notamment l'ajout d'une machine virtuelle pour exécuter du code protégé, afin de compliquer le travail des crackers. Une machine virtuelle, c'est un outil qui permet d'exécuter du code sous une autre forme que le code machine, un genre d'émulateur basique. Par exemple, Java utilise une machine virtuelle pour exécuter le code stocké dans un fichier .class. Pour comprendre le programme, il faut savoir interpréter ce code, qui est différent du code machine standard, d'où une difficulté supplémentaire. Reste à savoir si cela sera suffisamment efficace pour décourager les meilleurs crackers. Les paris sont ouverts, le prochain SafeDisc tiendra-t-il 1 jour, 1 semaine ou 1 mois ? (pas plus, faut pas déconner quand même)

UNE EXCLU, UNE VRAIE!

Vous devez en avoir l'habitude si vous nous lisez depuis le premier numéro, nous avions coutume de placer une exclusivité bidon parmi toutes nos news 100% non exclusives puisque pompées sur le net. Hors, il n'y en avait pas dans le numéro 4! Je suis sûr que vous êtes nombreux à vous demander pourquoi, même si personne ne semble l'avoir remarqué. Et bien, sachez qu'il y avait une vraie exclu exclusive de prévue, mais qu'elle n'est pas passée à cause d'une sombre histoire de fichier mal transmis. Dommage, vous l'avez raté donc.

LA RIAA A-T-ELLE LU LA LICENCE?

Sharman Networks a changé sa licence d'utilisation du logiciel sur la nouvelle version de Kazaa afin d'éviter qu'une tierce personne, au hasard la RIAA, abuse du réseau. En effet, si l'on observe attentivement la licence complète de Kazaa, on y lit qu'il est formellement interdit de s'en servir pour obtenir des renseignements sur les utilisateurs ou stocker leurs informations personnelles pour ensuite les utiliser contre eux. La RIAA ne pourrait donc plus attaquer les internautes car il lui serait légalement impossible de les identifier. Mais il est difficile de savoir si cette mesure va avoir l'effet escompté. Je doute que ces changements tiennent la route devant un tribunal, le juge risquant de ne pas tenir compte des modifications de la licence de la défense. Il faudra attendre de voir si un accusé ose sortir cet argument avant de savoir s'il est effectivement valable. En tout cas, cela prouve que Kazaa est bien décidé à faire tout son possible pour bloquer la RIAA, afin de mettre fin à la mauvaise réputation que lui ont apportée les récents procès.

RUSE D'ALLIGATOR

Gator, cette saleté de spyware qui n'a besoin que d'un clic pour polluer définitivement votre ordinateur, vient d'inventer un nouveau truc vicieux pour vous baiser discrètement. Se rendant compte que de plus en plus, Gator rimait avec "à mort" chez les internautes, ils ont décidé de renommer leur cacagiciel en "Claria". Peut-être qu'ils vont même remplacer leur croco par une délicieuse créature en petite tenue, promettant des merveilles à qui l'installera? Je ne saurai que trop vous le déconseiller, car Claria, c'est elle qui vous enc****a.

OUPS, ON AVAIT OUBLIÉ

L'image de Microsoft en prend encore un coup avec une bourde bien de chez eux. Ils ont tout simplement oublié de renouveler le nom de domaine hotmail.co.uk! Résultat, nos amis (c'est juste une façon de parler) grands-bretons qui ne savent pas que hotmail.com existe toujours sont, à l'heure d'écrire cette news complètement inutile qui n'intéresse personne, incapables de lire leur précieux mail. Pourquoi je vous raconte ça? Parce que ça serait quand même dommage de rater une si bonne occasion de nous moquer de nos amis de Microsoft.

UNE FAILLOUNETTE DE PLUS

Le service d'affichage de messages de Windows est une véritable plaie… En plus d'être utile uniquement aux spammeurs, une faille critique y a été découverte: elle permet l'exécution de code arbitraire à distance, grâce à une vulnérabilité de type buffer overflow. Si vous avez installé le patch depuis Windows Update, bloqué le service par une des méthodes décrites dans le Pirat'z numéro 3, ou vous êtes abonné d'AOL, normalement, vous n'avez pas pu être hacké. Dans le cas contraire, paniquez. Euh, et si vous êtes abonné d'AOL, paniquez quand même.

P2P : LA CULPABILITÉ IMPOSSIBLE À PROUVER

En marge de l'affaire contre Sarah Ward (lire notre news sur le sujet), un document technique publié sur un site australien démontre les faiblesses des méthodes utilisées pour confondre les utilisateurs de P2P. De très nombreuses failles de sécurité sur les logiciels d'échange de fichiers rendent en effet impossible l'identification à 100 % de l'utilisateur. Or, pour conduire une action en justice, le suspect doit être clairement identifié.

UN LOGICIEL D'ENQUÊTE POUR TOUS LES FLICS D'EUROPE

Les policiers de tous les pays européens disposeront bientôt d'un cadre légal commun pour enquêter. La Commission vient en effet de recommander l'utilisation de procédures " types " et surtout d'un logiciel d'aide à l'enquête. Baptisé CCAT, ce soft indique à chaque étape de la recherche de preuve les procédures à exécuter et les décisions à prendre. L'objectif est d'éviter que les preuves numériques soient invalidées devant les tribunaux, comme c'est aujourd'hui très souvent le cas.

STARFORCE COUPÉ DANS SON ÉLAN

StarForce est une sympathique compagnie développant des protections CD, dont on vous a déjà causé dans Pirat'z à quelques reprises. Rappelons que leur dernière protection (la version 3.0), censée bien sûr être à l'épreuve de tous les logiciels de copie, graveurs et crackeurs du monde, a bien sûr été crackée par les groupes pirates, même si la plupart des logiciels de copie ont effectivement des soucis avec (mais des solutions devraient finir par arriver). Bref, ce qui était marrant avec StarForce, c'est qu'ils avaient commencé une newletter mensuelle où ils parlaient des différentes protections, et comparaient combien de temps il avait fallu à tel jeu pour se faire cracker. Lorsque les jeux protégés par SF3 ont commencé à sortir et se faire cracker, ce tableau comparatif a soudainement disparu, et d'ailleurs la dernière newsletter date de … juin. Depuis, plus de nouvelles de cette initiative, censée officiellement informer des dernières avancées en matière de protection, mais paraissant plutôt servir de propagande aux produits StarForce. Bizarre ;-)

WEB CHINOIS : OUI AU SEXE MAIS NON À LA POLITIQUE

C'est le premier sujet de conversation en ce moment en Chine : la jolie Mu Zumei, 26 ans, qui raconte ses ébats sexuels sur Internet est-elle une s... ou une visionnaire libératrice ? Féministe rebelle pour les uns, débauchée pathétique pour les autres, la jeune Cantonaise publie sur son site web le nom de ces nombreux amants, des hommes mariés pour la plupart d'entre eux, et décrit en détail ses nuits d'amour. " Pour moi, faire l'amour est un hobby " dit elle.
Pas de quoi choquer pourtant les très puritaines autorités chinoises, qui profitent du phénomène pour cultiver une image de modernisme. Rappelons qu'une autre jeune internaute chinoise, Liu Di, 22 ans,étudiante, croupit toujours en prison depuis un an pour s'être gentiment moquée du parti communiste sur Internet.

RIAA PAS TAPER MOI

NPD Group a publié une étude montrant que les poursuites de la RIAA avaient atteint leur objectif. En plus de faire diminuer le nombre d'utilisateurs des réseaux P2P, plus d'un million de foyers américains auraient effacé leur collection entière de MP3 au mois d'août. Ils ne leur apparemment pas demandé, malheureusement, si c'était effectivement à cause de la RIAA, mais c'est ce que NPD Group affirme, et je veux bien les croire. Ça ressemble bien aux Américains, ça, d'effacer les MP3 au lieu de désinstaller Kazaa.

QUESTION DE LOGIQUE 1

Sachant qu'au Vietnam MS Windows coûte en moyenne 3 mois de salaire, est-il normal que ce pays soit celui qui connaît le plus fort de taux de piratage (97 %) ? Réponse : Oui.

PIRATAGE FOR EVER

" Les cd audio ne pourront jamais être efficacement protégés " C'est ce qu'affirme très sérieusement un informaticien de l'Université Princeton au New Jersey, John Halderman. Selon cet expert, la seule protection vraiment efficace contre la copie serait de baisser radicalement le prix des CD. Cette thèse est de plus en plus prise au sérieux par les majors aux Etats-unis, où 95 % de la population avoue dans un sondage récent Connaître quelqu'un qui a copié au moins une fois un CD (contre 20 % seulement pour un logiciel ou jeux vidéo).

321 ZÉRO !

Parmi les procès qui nous passionnent en ce moment de l'autre côté de l'Atlantique, il y a bien sûr celui contre McDo parce que ça fait grossir les gens, mais aussi celui qui oppose 321 Studios à l'industrie du cinéma américain. Le motif du désaccord: le logiciel DVD X Copy développé par la compagnie, et destiné à copier les DVD. Ce logiciel n'a rien de fantastique, vous pouvez trouver partout des outils gratuits pour copier vos DVD, mais ça a été la victime désignée par les studios de cinéma pour payer pour tous les autres. Dans la première décision officielle concernant ce cas, le "Copyright Office" américain a estimé que DVD X Copy était illégal, ce qui n'arrange pas trop les affaires de 321 Studios. Plus grave, cette décision risque de menacer le droit à la copie de sauvegarde aux USA, droit qui était encore a priori sauvegardé par la notion de "Fair Use" dans le DMCA. Encore plus grave, cela risquerait d'empêcher des milliers d'Américains de copier librement les DVD qu'ils louent quand même pour 3$, et c'est sans compter le prix du DVD-R. Quelle honte!

QUESTION DE LOGIQUE 2

Sachant que le gouvernement américain a exigé que le Vietnam réduise ce taux de piratage pour entrer dans l'Organisation Mondiale du Commerce en 2005 qui devrait en profiter directement ? Réponse : Microsoft

OH MON DIEU, LES ÉTUDIANTS PIRATENT!

C'est en gros le message du BSA, qui ont publié une nouvelle étude montrant que 89% des étudiants dans 1000 collèges et universités américains avaient déjà piraté des logiciels. Un chiffre qui semble les alarmer, mais qui ne devrait pourtant pas les surprendre, tant il est connu que les universités sont des lieux privilégiés pour la copie de logiciels. Selon le BSA, copier c'est mââââl, même pour les étudiants, et si on ne leur apprend pas dès leur plus jeune âge à ne pas pirater, ils risquent de continuer plus tard. Mouais, moi je voudrais une autre étude pour me prouver ça. Un autre argument qui me paraît plus vraisemblable serait de reconnaître que les étudiants n'ont souvent pas un rond pour se payer des licences Windows et Office, et que le BSA et Microsoft devraient se réjouir qu'ils les piratent au lieu de se tourner vers Linux. Comme ça, ils les achèteront plus tard lorsqu'ils les utiliseront dans leur compagnie. Ils se rendront sans doute compte de leur erreur un jour et passeront à Linux, mais ils l'auront au moins acheté une fois.

VOLEUR DE CODE, UNE PROFESSION EN DEVENIR

Après le bruit qui a entouré l'affaire du vol du code d'Half Life 2, c'est au tour d'une petite compagnie du Texas, Alibre, d'avoir affaire à un vol du même genre. Il s'agit de son logiciel, Alibre Design, qui aurait été emprunté par un ex-employé et redistribué en Russie sous le nom de "RaceCAD". Ce qui est marrant, c'est que le voleur a proposé à la compagnie d'arrêter de distribuer la version anglaise en échange de la version russe. Bizarrement, Alibre a refusé. Et s'apprête maintenant à lancer la mafia russe à ses trousses.

VIVE L'ÉDUCATION CIVIQUE !

Aaah, je me souviens avec nostalgie de mes cours d'éducation civique… L'assemblée nationale, le président, le pouvoir exécutif ou législatif, tout ça, qu'est-ce que c'était chiant, mon dieu… Ils ont de la chance aux USA, ils vont avoir droit à de nouveaux cours bien plus intéressants, car ça va parler… de piratage! C'est en effet la MPAA, l'industrie du film américain, qui a décidé de donner 100000$ pour faire passer leur message anti-piratage à 900000 jeunes américains. Ce sont des enseignants volontaires qui assureront ces cours. Ce joli programme s'inscrit naturellement dans le plan de campagne de la MPAA, qui veut éduquer les jeunes afin de leur apprendre à ne pas pirater. Ça a l'air plutôt bien, mais ça soulève quand même certaines interrogations. Notamment, le contenu de ces cours ne sera-t-il pas trop orienté en faveur de la MPAA, en "oubliant" par exemple de parler du droit de "Fair Use"? Les plus paranos comparent déjà cette initiative à l'endoctrinement stalinien de la jeunesse. Vénérera-t-on bientôt le portrait de Georges Lucas dans les classes?

LES PIRATES SONT VIEUX

Selon une étude canadienne, 24% des utilisateurs de peer-2-peer européens sont âgés de plus de 45 ans. Les 18-24 ans ne représentent que 16% contre 23 % pour les 35-44 ans. En France, pays des vieux, les plus de 45 ans représentent 32 % des utilisateurs, contre 22 % en Allemagne et 20 % en Angleterre. "Ces statistiques contredisent l'idée reçue selon laquelle les teen-agers sont les plus grands consommateurs de musique sur Internet" estime Leanne Sharman, vice-présidente des ventes et du marketing de Mp3.Com, commanditaire de l'enquête.

LES FRANÇAIS DERNIERS MONDIAUX DU P2P

Selon une étude très sérieuse de la société Digital intelligence, les Américains représentent plus de 50 % des utilisateurs du réseau P2P. Les Suédois arrivent en deuxième place avec près de 25 % de la population du logiciel. Presque derniers, les Français ne représentent que 1,22 % des utilisateurs de Kazaa. Petits joueurs...

PLUS DE SÉRIES TV SUR LE NET?

Dans les milieux warez du net, on trouve bien sûr des jeux, des films, des pdf de Pirat'z, mais aussi des séries télé. Notamment les séries américaines, que le reste du monde n'a souvent pas envie d'attendre plusieurs années. Il existe donc des groupes pirates spécialisés dans les séries télé, se livrant une guerre sans merci pour être les premiers à mettre sur le net chaque épisode, souvent quelques minutes à peine après leur diffusion… voire avant dans certains cas. Evidemment, ça ne fait pas trop plaisir aux chaînes de TV, car les groupes enlèvent systématiquement les pubs (et il y en a beaucoup aux USA). Et comme il s'agit de la source de revenus principale des chaînes publiques, Houston a un problème. La solution imaginée? Ajouter au signal vidéo un "flag" indiquant qu'il ne doit pas être copié. Tous les appareils de copie numérique vendus aux USA devront reconnaître ce flag d'ici juillet 2005, et interdire la copie lorsqu'il est présent. À votre avis, combien de temps faudra-t-il pour avoir un crack du logiciel de capture, ou du matériel piraté?

MUSIQUE "GRATUITE" À L'UNIVERSITÉ

Actuellement, dans les universités américaines, l'un des gros soucis est de savoir comment empêcher les étudiants de télécharger allègrement (et illégalement) leurs MP3 sur Kazaa. Et la solution s'appellerait… Napster ! Avec son retour sur le devant de la musique en ligne légale, Napster annonce en effet un accord assez révolutionnaire avec l'université américaine de Penn State. Les étudiants pourront écouter de la musique gratuitement, de façon illimitée. Ils pourront la télécharger sur 3 (trois!) ordinateurs différents. Par contre, s'ils veulent garder un morceau plus tard ou le graver sur CD, ils devront débourser la somme de 99 cents. Le principe est intéressant, mais un autre point de l'accord risque de faire grincer des dents : le coût de l'opération est prélevé sur l'argent donné par les étudiants en début d'année. Chaque étudiant va donc payer pour un service qui ne l'intéresse pas forcément. C'est vrai, quoi, je suis sûr qu'il y en a qui préféreraient pouvoir télécharger des jeux gratuitement, et pas des MP3! Voire des films de c**, mais ça, chut…

PRENEZ EXEMPLE

Lorsque vous faites quelque chose de mal sur votre ordinateur, comme scanner une université, hacker une machine ou regarder un film XXX, et que vous êtes démasqué, vous voilà bien embêté. Surtout dans ce dernier cas, d'autant plus que je n'ai rien à vous suggérer, sinon de vous rhabiller. Mais pour les autres, il est une excuse qui fonctionne souvent assez bien: il suffit de dire "ce n'est pas moi, c'est quelqu'un qui a installé un cheval de troie et utilisait mon ordinateur à distance". Un Américain de 19 ans a ainsi pu être acquitté d'une attaque de Denial of Service lancée contre un ordinateur de la base militaire de Houston, Texas. L'histoire ne dit pas s'il avait bien préparé son coup et qu'il y avait effectivement un cheval de troie sur sa machine, ou si l'accusation a été incapable de prouver qu'il n'y en avait pas, mais en tout cas il s'en est sorti indemne. Remarquez, peut-être même qu'il était innocent, mais ça, personne ne semble vraiment vouloir le considérer, la conclusion des experts étant que le système de collecte des preuves doit être amélioré.

QUESTION DE LOGIQUE 3

Sachant que les Vietnamiens ont accepté de réduire leur taux de piratage en équipant d'ici 2005 toutes les administrations, tous les services publics et 5000 écoles de logiciels Open Source, qui, finalement, n'en profitera pas ? Réponse : Microsoft

LA PEUR PAYE

1,4 de foyers américains ont nettoyé leur disque dur de tous fichiers musicaux durant le seul mois d'août dernier soit près de trois fois plus qu'au mois de mai dernier. Cette subite et estivale frénésie de ménage vient de la peur suscitée par les actions spectaculaires des maisons de disque contre les downloaders de musique en ligne. C'est un institut d'étude américain qui publie ce chiffre spectaculaire, tiré d'une enquête réalisée auprès de 40 000 internautes. En outre, selon cette étude, la fréquentation des sites P2P serait en chute libre et le nombre de morceaux téléchargés en baisse de 9 % en deux mois, entre août et septembre.

LE HACK FACILE AVEC EMULEZ !

DO IT ! FAUT-IL TOUT PARTAGER ?

On va voir qu'avec des outils standards de P2P, on peut accéder facilement aux fichiers personnels de certains utilisateurs. Alors, avec eMule par exemple, quels sont les fichiers système que l'on va pouvoir récupérer et comment ?

Pour commencer à bien pratiquer toutes les techniques de hack, on croit parfois qu'il faut maîtriser des outils complexes, créer ses propres programmes et en baver 200 nuits pour avancer, faire évoluer son niveau ...

Tous mes potes le disent, il faut utiliser Linux, avoir les yeux globuleux et les marques du clavier sur le front !

Regardons si il n'existe pas là, sous nos petits doigts malicieux, un programme très répandu, qui pourrait nous ouvrir quelques portes, voire nous faire un peu mieux connaître ce monde obscur :-)

Bon, arrêtons ce suspense intenable, quel est donc ce merveilleux outil ?

Le voici en images :

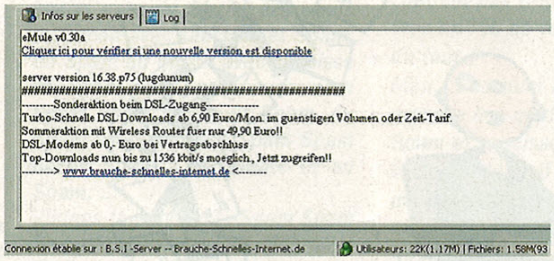
"Nonnnnnnnnn", je vous entends dire d'ici, pas eMule ! Et bien si, et passons tout de suite à la pratique.

Etape une, comme d'habitude dans votre utilisation quotidienne de ce bel outil, vous lancez la bête et vous vous connectez au serveur le plus proche (ou le plus fourni en softs et mp3z de tous bords, bande de vautours ?)

Ca donne une truc de ce genre dans la fenêtre de connexion et dans les différentes fenêtres associées :

- On peut alors voir le nombre de serveurs potentiels :

- Le serveur actuel qui me permet d'entrer dans la danse des échanges de fichiers :

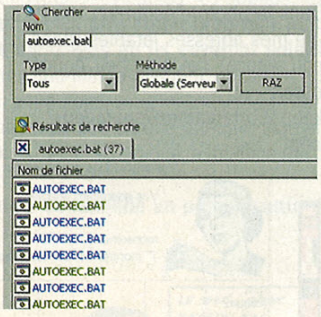


- Et enfin mon adresse IP, mais bon jusque là vous suiviez déjà pas mal, non ?

Vous êtes donc connectés avec eMule, tout va toujours bien, nous allons pouvoir passer au coeur de la manipulation à réaliser.

Vous allez maintenant faire comme d'habitude, aller dans la rubrique recherche, et au lieu de taper "madonna", "gamez" ou "Jean-Luc Godard", changez un peu et tapez plutôt "autoexec.bat".

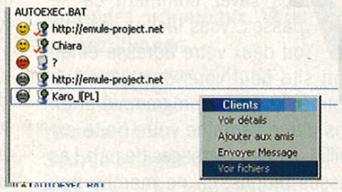
Et là, comme par magie vous allez vous retrouver sur au moins une bonne vingtaine de fichiers prêts à être chargés depuis des utilisateurs généreux ...



Là vous me direz, ok ça devient sympa, mais je vais faire quoi de ces jolis fichiers autoexec.bat qui traînent ?

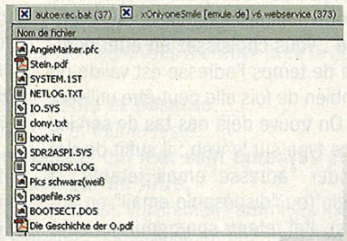
Exact, ce n'est effectivement pas dans ces fichiers là que vont se trouver les infos les plus intéressantes.

Poursuivons la manip et lançons le téléchargement de quelques autoexec.bat, mais au lieu d'attendre les chargements, on va utiliser le clic droit magique et choisir l'option " Voir Fichiers " sur l'utilisateur qui partage son autoexec.bat.



On obtient alors au minimum une fois sur deux la liste des fichiers qui s'affiche sans problème dans la fenêtre de recherche !

Et dans ces cas là, les fichiers ne sont plus uniquement des mp3



et autres mpg !

Les boot.ini, io.sys, bootsect.doc, config.sys, ... se laissent regarder, télécharger et analyser !!!

Je vous laisse maintenant libre de poursuivre dans cette voie ou une autre en fonction des pistes que votre imagination pourra vous suggérer.

Imaginons tomber sur un fichier de mots de passes partagés ... des codes qui traînent ...

Une brève explication s'impose tout de même.

Si ce genre de détournement est possible c'est que les différentes étapes réalisées jusqu'ici exploitent des " failles " cumulées ; le partage d'un répertoire c:\> au lieu d'un répertoire dédié au partage des fichiers eMule, l'autorisation de voir les fichiers d'un utilisateur eMule au lieu de voir uniquement les fichiers en cours de partage, ...

Malheureusement cette faille fait partie du domaine le plus prolifique de la sécurité sur Internet, encore plus célèbre que les bugs de Krosoft : les failles liées au facteur humain.

BONNE CHASSE.

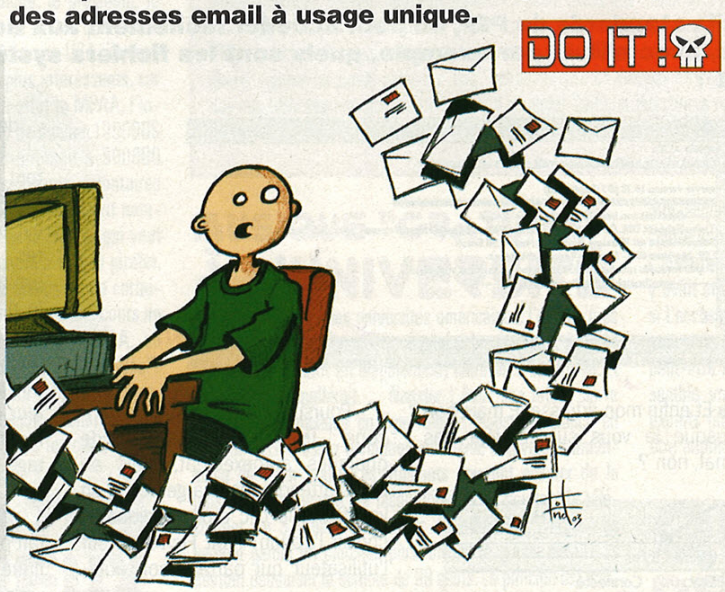
LA LÉGALITÉ DANS TOUT ÇA ?

La loi interdit deux choses (entre autre...):
1.de posséder, et a fortiori de distribuer ou partager, des contenus dont on a pas obtenu les droits,
2.d'accéder à des ressources protégées sans autorisation.
Pas de problème avec ce premier point : les fichiers système comme autoexec.bat ne font pas l'objet d'un copyright. Ensuite, vu que ces fichiers sont explicitement partagés et publiques, on ne contredit pas le deuxième point. Alors qu'il est illégal de télécharger des films ou des mp3, il est parfaitement légal de télécharger des autoexec.bat partagés " volontairement " par d'autres utilisateurs.
Mais attention ! Ce que vous faites avec les fichiers téléchargés peut devenir illégal. Vous n'avez par exemple pas le droit d'accéder à des services avec des mots de passe récupérés de cette manière ou d'exploiter des informations personnelles.

L'ADRESSE EMAIL JETABLE

UNE MANIÈRE INTELLIGENTE DE LUTTER CONTRE LE SPAM

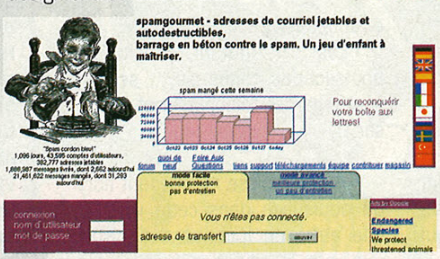
Vous pouvez vous débarrasser de la majorité des problèmes de SPAM en utilisant des adresses email à usage unique.



Vous savez comment ça se passe... Vous lâchez une fois ou deux votre adresse email sur un site pour vous enregistrer ou pour télécharger un programme et en moins d'une semaine votre boîte est assaillie par des messages de pub. Les adresses bidons, ça ne marche pas toujours. Et les comptes-poubelles que l'on crée régulièrement sur hotmail ou yahoo, ça va un moment.

Et bien il existe une solution très maligne pour remédier au problème du SPAM à la racine : les adresses jetables. Elles vous permettent de ne donner sur les site que des adresses qui n'ont pas de valeur pour les spameurs et vous minimisez la nuisance potentielle : vous choisissez en effet combien de temps l'adresse est valide ou combien de fois elle peut-être utilisée.

On trouve déjà des tas de service de ce type sur le web : il suffit de demander "adresse email jetable" à google (ou "disposable email" en anglais). J'ai retenu spamgourmet.com pour l'ingéniosité de ses services et le design chaleureux du site.



Spam Gourmet offre un service de redirection. Ça veut dire qu'il faut d'abord s'inscrire et donner une adresse email valide. Là, pas de soucis, ils ne vont pas vous envoyer quoi que ce soit à cette adresse, ni la communiquer à quiconque. Une fois enregistré, il n'y a plus rien à configurer et vous pouvez utiliser leur service. Le principe est le suivant : lorsqu'un site vous demande une adresse email, vous lui donnez une adresse du type motclef.3.priatgamez@spamgourmet.com. Ici, piratgamez est votre login sur spamgourmet.com, motclef est un mot que vous avez choisi (par exemple le nom du site) et 3 est le nombre de fois que l'adresse pourra être utilisée. Ça veut dire que le site auquel vous avez donné cet email ne pourra l'utiliser que 3 fois pour vous contacter (par exemple pour recevoir la confirmation de votre inscription). Les trois premiers emails seront ainsi redirigés vers votre adresse privée, et tout le reste sera balancé dans le néant.

Dans la photo d'écran, on voit la liste de mes adresses jetables (dans le menu avancé). J'ai, il y a peu, donné l'adresse : diskkeep.2.priatgamez@spamgourmet.com à un site pour télécharger une version d'évaluation de Disk Keeper. En quelques jours, il m'ont déjà envoyé 4 messages, mais je n'en ai reçu que deux dans ma boîte (et n'en recevrai plus jamais d'autre).

Les petits malins me diront que les faiseurs de SPAM n'ont qu'à exploiter ce service et envoyer leur messages publicitaires en utilisant des nouveaux mots-clés aléatoires. Franchement, je n'y crois pas, parce que de toute évidence, ils ne vont pas se casser la tête pour trouver des adresses dont ils sont sûrs que les propriétaires ne désirent pas recevoir de publicité. Mais Spam Gourmet a prévu quelques options pour les plus paranoïaques. On peut par exemple définir des mots qui doivent apparaître dans les nouvelles adresses jetables pour qu'elles fonctionnent.

Notez que si vous avez besoin de réutiliser une adresse dont la limite a déjà été dépassée, il est possible de réinitialiser sont compteur. Il y a encore une foule d'autres fonctionnalités de ce style, que je vous laisse découvrir sur le site.

Spam Gourmet fournit ce service gratuitement, sans publicité. On peut se demander pourquoi. En fait, ils se servent des messages qu'ils détruisent pour récolter des données statistiques sur le SPAM. Vous pouvez d'ailleurs vous-mêmes faire quelques expériences avec ce système. Il est par exemple intéressant d'observer, si vous n'utilisez qu'une adresse par site, de quel source un faiseur de SPAM a obtenu votre adresse. Vous pouvez aussi vérifier qu'un site respecte ses engagements de ne pas exploiter votre adresse. Ou encore, vous pouvez voir si un forum est exposé aux moissonneurs d'adresses, en y laissant une adresse jetable.

Vos statistiques de messages: 16 transférés, 3 mangés. Vous avez 7 adresse(s) jetable(

Vos addresses jetables

rechercher: [ ]
[ ] montrer les adresses cachées chercher retourner au mode avancé

mot (cliquez pour éditer)	maximum	restant	transférés	mangés	création (PST)	adresse
diskkeep	2	**0**	2	2	2003-10-24 12:36	diskkeep.2.piratgamez@spamgourmet.com
seloger	20	20	2	0	2003-09-11 09:17	seloger.20.piratgamez@spamgourmet.com
rplayer	2	**0**	2	1	2003-08-14 13:20	rplayer.2.piratgamez@spamgourmet.com
cinecourts	8	6	2	0	2003-06-01 08:41	cinecourts.8.piratgamez@spamgourmet.cor
card	1	**0**	1	0	2003-05-31 06:54	card.1.piratgamez@spamgourmet.com

'Z

C'EST PAS JUSTE !

Quelque part pas loin, se trouve la newvs la plus inutile du mois, à propos de Microsoft et de son trou de mémoire lors du renouvellement de hotmail.co.uk. Là où ça se corse, c'est que quelqu'un en a profité pour se l'approprier! Selon The Register, cet individu était en fait bien gentil et a voulu rendre le domaine à Microsoft, mais Billou aurait fait la sourde oreille, jusqu'à ce que l'affaire soit rendue publique. Finalement, Microsoft devrait maintenant avoir récupéré son dû. Dommage, ça aurait été plus drôle si c'était moi qui l'avais eu...

GAME OVERNET

Sortie officielle ce mois-ci d'Overnet 0.51, le frère ennemi d'eMule 0.30. Cette dernière version, qui sort sans eDonkey, apporte notamment une refonte de la page des fichiers partagés permettant de lancer une vidéo directement ou d'ajouter un fichier en le faisant glisser. Appréciable : la possibilité de désactiver Horde. Overnet essaye ainsi de s'imposer comme un Kazaa haut de gamme.

LE (BEAU) CHEMIN DE LA LÉGALITÉ SEMÉ D'EMBÛCHE

Deux étudiants du fameux MIT (Massachusetts Institute of Technology) ont eu l'idée de proposer un service de libraire audio via le système de télé par câble de l'école. Légale, la gestion des droits reposait sur des partenariats signés avec des représentants d'éditeur. Or, l'un d'entre eux, la compagnie Loudeye, de Seattle, n'avait en réalité pas de licence lui donnant droit de revendre de la musique ! Le MIT a immédiatement stoppé son projet. Un geste apprécié par la plupart des Majors qui voient dans cette décision un grand pas franchi vers la légalisation des échanges.

AUTOUR DU SPAM

MONTY PYTHON FLYING CIRCUS

Je ne peux pas m'empêcher de parler du fameux sketch des Monty Python. Le SPAM (Spiced Pork And Ham), ça s'achète en grande surface : c'est une sorte de corned-beaf bon marché, à la réputation douteuse en Grande-Bretagne. Dans les années 70, les Monty Python, un groupe de comiques anglais délirants et monstreux, ont écrit un sketch sur cette dure réalité de la gastronomie.

Ca ressemble à ça :

[...]
Man : Bien, que nous proposez-vous ?
Waitress : Eh bien, il y a des oeufs au bacon, des oeufs au bacon avec saucisse, des oeufs avec du Spam, des oeufs au bacon avec du Spam, des oeufs au bacon avec saucisse et Spam, du Spam au bacon avec saucisse et Spam, du Spam avec oeuf Spam Spam bacon et Spam, du Spam avec saucisse Spam Spam bacon Spam à la tomate et au Spam, ...
Vikings (en choeur) : Spam Spam Spam Spam...
Waitress : ...Spam Spam Spam oeufs et Spam, Spam Spam Spam Spam Spam haricots Spam Spam Spam...
Vikings (chantant) : Spam ! Délicieux Spam ! Délicieux Spam !
Waitress : ...et du homard Thermidor en sauce Mornay, servi à la provençale avec échalotes et aubergines, garni de pâté truffé, flambé au Cognac avec un oeuf à cheval et du Spam.
Woman : Auriez-vous quelque chose sans Spam ?
Waitress : Eh bien, il y a le Spam oeuf saucisse et Spam, ça ne contient pas trop de Spam.
Woman : Je ne veux pas de Spam du tout !
Man : Pourquoi ne peut-elle pas prendre des oeufs au bacon avec Spam et saucisse ?
Woman : Mais il y a du Spam là-dedans !
Man : Pas autant que dans le Spam oeuf saucisse et Spam, non ?
Vikings : Spam Spam Spam Spam... ETC...

A la fin, les dialogues sont innondés par les élucubrations des Vickings et des autres personnages et on n'entend plus les personnages principaux. Vous comprenez l'image.
La chanson des Vikings :
http://www.mailmsg.com/sounds/spam-song.wav
Source images :
http://www.halte-spam.com

DES CHIFFRES ET DES MAILS

Une étude américaine de PIP (Pew Internet & American Life Project) donne des chiffres accablants sur le sujet.

25 % des sondés disent que le SPAM fait qu'ils utilisent moins le courrier électronique.
C'est vraiment un fléau. Ça signifie que l'on ne va presque plus recevoir de blagues par email. Donc les employés de bureau vont travailler moins, parce qu'ils déprimment plus.
52 % des sondés disent que le SPAM réduit la confiance qu'ils donnent à l'email en général.
C'est pas forcément un mal. De quand date le dernier message que Bill.Gates@microsoft.com vous a envoyé avec la dernière version de Windows (windows.exe) ?
70 % des sondés trouvent que le SPAM a rendu la vie sur Internet désagréable et pesante.
C'est un peu injuste. Il y a aussi les bandeaux publicitaires, les popups, les spywares et tout le reste.
30 % des sondés ont peur que leur filtres anti-spam bloquent aussi les emails qui leur sont adressés et 23 % des sondés ont peur que les messages qu'ils envoient soient bloqués par un filtre.
Simple. Il faut mettre en place des filtres anti-filtre-anti-spam, qui sont capables de trier les vrais emails parmi les messages marqués comme SPAM. Et puis, entre nous, vous ne trouvez pas que ça constitue une excuse de premier choix : "Ah non, je ne savais pas... Ton message a dû être bloqué par mon filtre anti-spam. " Héhé.
Sinon, évitez les phrases du style : "Alfred, pour cette peine, a rallongé ton pastis ? " Certains filtres savent même traquer le contrepet.
7 % des sondés avouent qu'ils ont déjà commandé un produit vanté dans un email qu'ils n'avaient pas sollicité.
Pas de commentaire.

'Z

BAD BIRTHDAY VIRUS !

Le 1er virus informatique de l'histoire est né il y a tout juste 20 ans. C'était à la fin du mois de novembre 1983, dans le labo d'un étudiant de l'université de Californie. Il s'agissait alors d'un simple " code " destiné aux plate- formes Vax 11/750 possédant la faculté de se reproduire lui-même dans des fichiers exécutables. C'est à un prof de la même université, Léo Adleman, que l'on doit la paternité du nom " Virus ".

AVOCAT DE LA RIAA, UNE AUTRE PROFESSION PHARE

C'est qu'ils doivent en avoir du boulot, ces pauvres avocats, avec le nombre de procès qu'ils lancent... Surtout lorsque tout ne se passe pas comme prévu, comme avec le fournisseur d'accès par câble Charter. Celui-ci semble vouloir faire comme Verizon et retarder au maximum le moment où ils devront dévoiler à la RIAA les noms de leurs 150 abonnés qui auraient téléchargé illégalement des MP3. C'est le cas aussi de Pacific Bell Internet, un autre fournisseur d'accès. Bref, encore et toujours des procès, ça commence à lasser...

KAZAA BIENTÔT PAYANT?

Depuis peu, Kazaa a mis sur le marché une version payante de son logiciel, qui offre évidemment d'autres services. Il est probable qu'il devienne complètement payant sous peu. Sharman Networks tenterait de faire payer les utilisateurs à chaque téléchargement afin d'éviter d'être traîné en justice par la RIAA. Les modes de paiement seraient la carte de crédit bien sûr, mais on aurait aussi la possibilité d'envoyer la facture au fournisseur, qui l'ajouterait au solde de notre facture internet. Oups, c'est que ma facture risque d'augmenter, on dirait :-/

DO IT !

PWL CRACK

CRACKER LES MOTS DE PASSE WINDOWS 95/98

Il est fréquent que l'on puisse obtenir des fichiers .PWL de Windows 95/98/Me. Nous allons voir à quoi ils servent et ce qu'ils contiennent. Nous allons également éprouver leur fiabilité et montrer comment on peut en cracker le mot de passe.

MODE REGIONALE

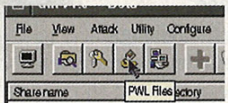
Les Américains et les Européens n'utilisent pas les mêmes logiciels de Peer-to-Peer. Selon une étude, les Américains ne jurent pratiquement que par Kazaa, qui arrive n'arrive pourtant que bon deuxième en Europe, après eDonkey. Ce dernier est particulièrement populaire pour le téléchargement de vidéos. Le marché du partage de fichiers a beaucoup évolué au cours des dernières années, et on peut ainsi remarquer des différences selon les régions. Toutefois, ce genre de logiciels P2P naissent très vite, mais meurent tout aussi rapidement. Alors il est probable qu'un jour, tout comme Gnutella, Kazaa soit chose du passé. D'un autre côté, il est aussi possible de renaître de ses cendres, comme Napster qui reprend du service ce mois-ci, ce qui inquiète les fournisseurs d'accès. Les logiciels de partage P2P, légaux ou non, génèrent en effet un trafic considérable qui leur coûte très cher en bande passante. Mais si c'est Napster qui vous inquiète, Messieurs les FAI, rassurez-vous, son cadavre sanguinolent ne devrait pas trop vous causer de problèmes.

LA CHARTE DU P2P

Toujours afin de se faire bien voir de la RIAA qui ne veut décidément pas les lâcher, les grands réseaux Peer-to-Peer (Kazaa, eDonkey, Grokster and co) ont décidé de se réunir et de réfléchir à une "charte du P2P" qui les mettrait à l'abri des poursuites. Cette charte comporterait des points comme l'obligation d'informer l'utilisateur de l'interdiction de partager des fichiers illégaux, et des poursuites qui pourraient en découler. C'est une initiative louable, mais il reste à voir si elle aura un impact réel sur les poursuites judiciaires.

Un script kiddie qui se respecte fait au moins ses 40 heures de brute force acharné par jour. Le brute force, c'est un procédé pour casser certains mots de passe, qui consiste à essayer toutes les possibilités. Ça paraît bête, mais c'est souvent la meilleure technique connue. Cependant, elle ne reste applicable, en pratique, que lorsque le champ d'exploration est assez restreint et lorsque, conjointement, le temps nécessaire à vérifier un mot de passe est raisonnable.

En général, on fait du brute force sur son ou ses ordinateurs, sur des fichiers de mots de passe qu'on a récupéré Dieu sait comment (Dieu a peut-être lu notre article sur eMuleZ, par exemple...). Avec les mots de passe qu'il a cracké, le brillant script kiddie peut accéder à de nouveaux ordinateur, d'où il télécharge de nouveaux fichiers password à cracker. Et ainsi de suite. Quelle vie excitante ! On va voir que cet exploit est à la portée du premier venu.



I. LA SÉCTION PWL FILES

LES FICHIERS PWL

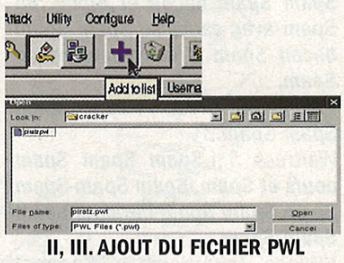
Vous êtes sans doute encore nombreux à utiliser Windows 95/98 (ou même Me, pauvres de vous). Les temps sont durs, les ordinateurs sont chers et on ne parle même pas du prix de Windows XP dans le commerce (et vous n'allez pas vous risquer à en utiliser une version pirate, pas vrai ?).

Bon, Windows 9x, c'est tout à fait utilisable et ça a l'avantage de ne pas nécessiter un ordinateur dernier cri pour tourner. Mais il faut avouer qu'en matière de sécurité, si l'ordinateur est en ligne, il y a des raisons de se méfier. Une des faiblesse les plus connues de ce système est la manière dont sont mémorisé certaines informations sensibles relatives à un utilisateur : les fichiers PWL (pour PassWord List).

Lorsque vous êtes en mode multi-utilisateur (quand vous devez entrer un mot de passe au démarrage), le système vous permet de stocker les mots de passe de votre FAI, de certains comptes, ou de disques réseau (lorsque vous cocher "mémoriser le mot de passe"), dans un fichier utilisateur.pwl. Ce fichier est crypté et protégé par votre mot de passe principal. Vous trouverez le votre dans le répertoire C: \Windows.

En d'autres termes, si quelqu'un arrive à se procurer votre fichier PWL et à le décoder, il obtient tous vos mots de passe cachés. Et peut-être que vous utilisez les mêmes mots de passe pour d'autres services plus importants. Vous voyez le problème ?

Il y a un moyen de désactiver la mémorisation des mots de passe dans ces fichiers. Il faut modifier la base de registres, avec regedit.exe. Il faut changer cette entrée et la mettre à 1 : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\DisablePwdCaching = 1.



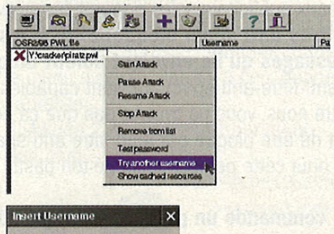
II, III. AJOUT DU FICHIER PWL

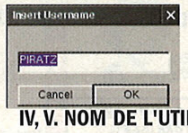
DÉCODER LES PWL

Il existe de nombreux programmes qui permettent de cracker le mot de passe d'un fichier PWL. J'ai choisi de présenter Cain1.0, parce que c'est une version Freeware. On la trouve ici : http://packetstormsecurity.nl/Crackers/Cain10b.zip

Vous pouvez aussi utiliser PWLTool, Cain2.0 ou beaucoup d'autres. Cain permet de faire d'autres choses que de simplement cracker ces fichiers. Ce programme permet par exemple de décoder les mots de passe (qui sont en mémoire) de l'utilisateur courant. Mais les reste de ses fonctionnalités ne nous intéressent pas ici.

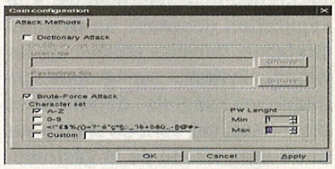
L'interface de Cain1.0 est assez sobre. C'est la partie PWL Files que nous allons utiliser (I). Il faut commencer par inscrire le fichier PWL que l'on veut cracker dans la liste (II, III). Il est ensuite nécessaire de donner le nom de l'utilisateur correspondant (IV, V). En général, le nom du fichier correspond au nom de l'utilisateur (tronqué à 8 caractères).





IV, V. NOM DE L'UTILISATEUR

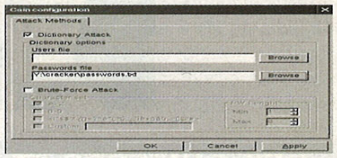
On choisit ensuite le type d'attaque, en cliquant sur le menu Configure : par brute force ou par dictionnaire. En mode brute force (VI), on doit définir l'ensemble des caractères sur lesquels la recherche va porter. On peut parier, par exemple, que l'utilisateur n'a choisit que des lettres (pas de nombre ou de signe), ce qui accélère nettement l'attaque (déjà qu'il n'y a pas de distinction entre majuscules et minuscules...).



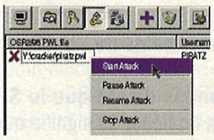
VI. MODE BRUTE FORCE

En mode dictionnaire (VII), on désigne simplement un fichier qui contient une liste de mots (un par ligne, on appelle ça une wordlist, cherchez sur google). La recherche va beaucoup plus vite, mais ça suppose que le mot de passe est un mot répertorié. On peut aussi utiliser un dictionnaire pour deviner le nom d'utilisateur.

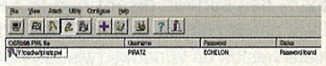
Ensuite, il ne reste plus qu'à lancer l'attaque (VIII), attendre (de quelques minutes à quelques heures) et apprécier le résultat (IX). Cain permet bien sûr d'obtenir la liste des informations confidentielles mémorisées dans le PWL, une fois cracké.



VII. MODE DICTIONNAIRE



VIII. LANCER L'ATTAQUE



IX. MOT DE PASSE CRACKÉ

MORALE

Vous avez pu vous convaincre qu'il est facile de s'attaquer à un fichier PWL et je pense que vous pourrez imaginer vous-mêmes comment un pirate peut se procurer ce genre de fichiers. Vous avez même les moyens d'expérimenter la force et la faiblesse de vos mots de passe. Vous arriverez alors probablement à la conclusion qu'un mot de passe court formé de lettres est rapide à casser, alors qu'un mot de passe long (au moins 8 caractères), composé de lettres, de chiffres et de signes prend tout de suite beaucoup plus de temps. On vous a déjà conseillé d'utiliser des mots de passes compliqués ? Et bien si vous utilisez Windows 9x, voilà une bonne raison de le faire.

Salut à Lord Zak, qui a inspiré cet article.

DE BAZANDE

DO IT !

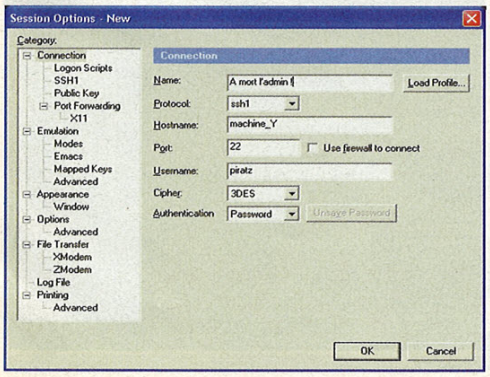
SAVOIR EXPLOITER LE SSH TUNNELING

Je ne vais pas vous parler d'une technique de hack révolutionnaire, mais d'une petite astuce qui peut être bonne à savoir pour contourner certains obstacles. Nous allons voir comment exploiter une connexion SSH pour créer un tunnel sécurisé servant à faire transiter vos données au nez et à la barbe d'un firewall. Oui, rien que ça !

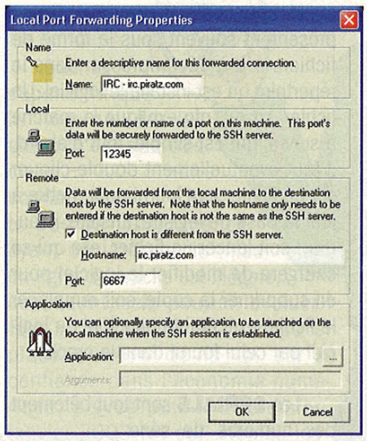
Bon, trêve de blabla technique, voyons exactement quel est le problème que l'on va résoudre, par un exemple pas si éloigné que ça de la réalité. Imaginez que vous êtes sur un campus d'université, et que votre ordinateur (X) est séparé de l'extérieur par un vilain firewall, qui notamment bloque les ports 6667 et Cie pour empêcher les élèves d'accéder à l'IRC. Par contre, il existe un ordinateur de l'université, nommé Y, sur lequel vous avez un compte, qui lui n'est pas bloqué vers l'extérieur (cet ordinateur pourrait aussi être extérieur à l'université).

Une première idée serait d'installer un proxy Socks sur Y, mais peut-être que vous n'avez pas la possibilité de faire cela, parce qu'encore une fois l'administrateur système, l'éternel ennemi des étudiants, a un peu trop restreint vos droits. Qu'à cela ne tienne, il est possible d'exploiter une simple connexion SSH (connexion genre telnet, mais sécurisée) pour utiliser la machine Y comme relais vers votre serveur IRC.... Comment ? C'est ce que nous allons voir tout de suite !

Nous allons utiliser SecureCRT, dont vous pouvez télécharger une version d'évaluation limitée à 30 jours sur www.vandyke.com/download/securecrt/. Il existe certainement d'autres logiciels capables de faire ce que nous allons faire, à vous de les trouver si SecureCRT ne vous convient pas. Installez puis lancez la bestiole. Sur la fenêtre "Quick Connect", cliquez sur "Cancel". Faites ensuite Alt-C puis Alt-N pour créer une nouvelle session. Dans "Hostname", mettez l'adresse IP de la machine Y. Dans "Username", rentrez votre login.



Cliquez ensuite sur "Port Forwarding", puis sur "Add" pour ajouter une redirection de port. Dans la section "Local", mettez dans "Port" le port que vous allez utiliser sur votre machine (à peu près n'importe quoi de plus petit que 65536 devrait fonctionner). Dans la section "Remote", cochez "Destination host is different from the SSH server", et dans "Hostname" mettez l'adresse du serveur IRC auquel vous souhaitez vous connecter. Dans "Port", ça sera bien sûr le port de ce serveur qu'il faudra mettre (pour l'IRC c'est généralement 6667). Enfin,



laissez vide le champ "Application".

Cliquez maintenant sur OK, encore OK, puis Connect pour vous connecter sur la machine Y. On va sans doute vous demander votre mot de passe, ainsi que d'accepter la clef du serveur (Y), ce que vous ferez bien gentiment. Une fois connecté, que reste-t-il à faire ? Rien du tout, tout est prêt ! Il ne reste plus qu'à lancer mIRC, et à spécifier comme serveur "127.0.0.1" sur le port 12345 (si c'est ce que vous avez mis comme port local dans SecureCRT). Et là, si le serveur affiche votre adresse IP au démarrage, vous devriez voir l'adresse de Y et non pas la vôtre, comme ceci par exemple :

Local host: Y.universite.fr (80.81.82.83)

ET C'EST PAS FINI

Ce petit article touche à sa fin, mais le principe de base que nous venons de voir offre bien plus de possibilités que simplement faire de l'IRC peinard. Une première chose à savoir est qu'il est ainsi possible de créer toute une chaîne de tunnels. Imaginons que vous vouliez vous connecter en utilisant la chaîne X -> Y -> Z -> Serveur IRC. Commencez par modifier votre session dans SecureCRT, en décochant "Destination host is different from the SSH Server" et en changeant le port en dessous en "54321". Ainsi, lorsque vous vous connecterez sur X:12345, la connexion sera redirigée sur Y:54321. C'est la première étape. La seconde est de rediriger Y:54321 vers le serveur IRC, en passant par Z. Cela se fait par une autre connexion SSH. Comme il s'agit de machines Unix ce n'est pas SecureCRT que nous utilisons, mais tout bêtement ce bon vieux SSH. Connectez-vous sur Y grâce à votre connexion SecureCRT. Tapez alors:

ssh -L54321:irc.piratz.com:6667 Z

où vous avez bien sûr mis votre véritable serveur IRC. Cette commande a pour effet de rediriger le port local (-L) numéro 54321 de Y vers le port 6667 de irc.piratz.com, en passant par la connexion SSH initiée avec Z. Ce qui réalise exactement la chaîne voulue ! En vous connectant par mIRC sur votre propre machine, port 12345, le serveur IRC va donc croire que vous êtes Z :

Local host: Z.universite.fr (80.81.82.84)

Vous voulez faire des chaînes encore plus longues, en rajoutant une machine T par exemple ? Facile, la ligne ssh ci-dessus sera à remplacer par :

ssh -L54321:localhost:54321 Z

et vous continuerez votre chaîne en vous connectant sur T à partir de Z par :

ssh -L54321:irc.piratz.com:6667 T

Maintenant que vous êtes capable de faire valser vos connexions partout sur le réseau, il ne vous reste plus qu'à trouver d'autres applications à cet outil bien pratique qu'est le tunnel... Sachant qu'une des premières applications est de sécuriser une connexion, les données transitant dans le tunnel étant cryptées. Par exemple, vous pouvez ainsi sécuriser la récupération de vos mails, si le serveur de mail est la machine Y, même si le serveur lui-même n'est pas sécurisé. Tiens, ça sera votre exercice d'application pour le prochain numéro !

ETVID

PEERCACHE ABANDONNÉ

On vous rapportait que la filiale hollandaise de Wanadoo expérimentait un nouveau logiciel du joli nom de PeerCache. Ce logiciel était censé réduire le trafic engendré par les utilisateurs de P2P, en stockant les fichiers sur les serveurs du fournisseur d'accès, qui pouvait ainsi les transférer directement à ses utilisateurs et par là même économiser une grande partie de la bande passante. Là où le bât blesse, c'est que les défenseurs des droits d'auteur ne voient pas ça comme une solution viable au problème, et au contraire dénoncent le fait que cacher - même temporairement - des fichiers illégaux est illégal. Ce en quoi ils n'ont pas tort, n'en déplaise aux adeptes de "je garde ma ROM 24h donc c'est légal". Devant les sourcils froncés et les doigts tendus provoqués par l'annonce de l'utilisation de PeerCache, Wanadoo a fait marche arrière, et PeerCache ne sera pas employé. Enfin, pas tout de suite, plusieurs autres fournisseurs étudiant actuellement le produit, pour trouver comment récupérer pour eux les téraoctets de jeux piratés qu'ils vont stocker.

BOURSICOTI, BOURSICOTA

Un jeune américain de 19 ans risque jusqu'à 20 ans prison pour avoir vendu des options de vente d'action. Le problème, c'est qu'il avait piraté le compte de l'acheteur (avec un keylogger) pour se débarasser de titres sans valeur. Ce n'est en fait pas la victime, mais la SEC (Securities and Exchange Commission) qui porte plainte pour fraude boursière, après avoir traqué le coupable. Le département de la SEC qui s'occupe d'Internet est à l'origine de plus de 400 actions judicaires depuis 1995. Ils n'avaient pourtant jamais rien vu de tel.

UTILISER LES CRACKS

Copier un logiciel, c'est facile, il suffit de graver le CD-ROM. Mais comment faire fonctionner la copie malgré la protection ? Une version démo bridée, c'est parfois insuffisant pour évaluer correctement un logiciel. Comment lui redonner toutes ses fonctionnalités ? Les solutions pour tous ces problèmes s'appelent cracks, serials, keygens...

KAZAA EN VACANCES

Il semblerait que les poursuites de la RIAA contre les utilisateurs de MP3 aient porté leur fruit. Selon une étude du cabinet Nielsen / Netrating, les partageurs de fichiers musicaux étaient moins nombreux durant l'été. En effet, Kazaa aurait perdu un peu plus de 40% d'audience et Morpheus 4% pendant l'été. Les autres logiciels de ce genre ne font pas partie de l'étude parce que leur taux d'audience était trop bas (aux USA évidemment). Voilà qui prouve que les gens prennent des vacances en été, un fait nouveau assez inexplicable.

LA RIAA SE FAIT DES AMIS!

Eh oui, encore une fois les aventures de la RIAA, qui cette fois-ci règle à l'amiable les poursuites intentées contre les utilisateurs de P2P. En effet, il semblerait qu'une cinquantaine de " poursuivis " auraient de leur plein gré accepté de verser une somme entre 2500 et 7500$ américains. L'entente stipule que les utilisateurs doivent détruire les fichiers téléchargés. Pour soutenir la RIAA, une association a été formée par les principaux éditeurs d'application P2P, association qui a pour mission d'éduquer, mais surtout d'informer les utilisateurs. P2P United (eDonkey, LimeWire, Bearshare, Morpheus et Blubster) développera une charte de bonne conduite, avant la fin de 2003, sur l'illégalité du partage de fichiers protégés par la loi sur les droits d'auteur. Tout le monde connaît évidemment cette loi, mais qui la respecte? Est-ce que cette association réussira vraiment à changer quoi que ce soit aux yeux des utilisateurs? Pourquoi Kazaa n'y figure pas? Autant de questions dont la réponse est attendue impatiemment par, euh, au moins 3 personnes.

Qui n'a jamais perdu son CD original de "remplacez ici par votre jeu préféré", et, se retrouvant contraint de le lancer à partir d'une copie de sauvegarde, s'est rendu compte avec stupeur que la protection l'empêchait de fonctionner ? Bon OK, pas grand monde, mais ce qui nous intéresse ici c'est de savoir comment on peut trouver des cracks pour éliminer ces protections et pouvoir enfin utiliser sans risque les CD originaux comme freesbees, parce qu'ils sont quand même plus design que des cédéroms vierges. Ceux qui verraient ici une incitation au piratage de logiciels, pour pouvoir copier puis utiliser gratuitement les jeux, mais aussi plein d'utilitaires, et même des outils de sécurité et de hacking, se trompent complètement car rappelons-le, c'est interdit par la loi.

Et ceux qui verraient de l'ironie dans cette dernière phrase sont probablement des étudiants anarchistes irrespectueux et irrécupérables qui n'ont même pas acheté Windows, aussi nous ne répondrons pas à cette perfide insinuation.

SUPPRIMER LES POP-UPS

Avant de commencer, réglons son compte au problème des pop-ups. Quand on se balade sur un site web de cracks, on se retrouve très vite encombré d'une multitude de petites fenêtres vantant les prouesses sexuelles de jeunes filles aguichantes. Impossible de ne pas se laisser distraire, il faut donc supprimer ces apparitions de fenêtres si on veut avoir une chance de rester suffisamment concentré pour télécharger un crack.

DEUX SOLUTIONS :

1. Utilisez le navigateur web gratuit Mozilla. La photo d'écran vous montre comment désactiver les pop-ups.

2. Utilisez un logiciel dédié, de préférence qui supprime également les publicités. Malheureusement ces logiciels sont payants. Quoique les pirates pourront essayer de trouver un crack... ;-)

CRACKS ET SERIALS : OU LES TROUVER

Les **CRACKS** sont de petits programmes à exécuter après avoir installé une copie du logiciel. Ils se présentent souvent sous la forme de fichiers .zip à décompresser dans le répertoire où est installé le logiciel. Un fichier .txt ou .nfo explique la marche à suivre, qui est simple. Tout d'abord, il faut éventuellement double-cliquer sur un fichier .reg fourni pour mettre à jour la base de registre. Ensuite, il faudra : soit lancer un fichier .exe qui se chargera de modifier le logiciel pour en supprimer la copie, soit remplacer le fichier exécutable principal du logiciel par celui fourni dans le crack.

Les **SERIALS** sont tout bêtement des numéros de série permettant d'activer un logiciel, de permettre son installation, ou de transformer une démo en version complète. Il est illégal d'utiliser un sérial sauf si vous avez perdu le numéro de série fourni lors de l'achat de votre logiciel.

Les **KEYGENS** sont des logiciels capables de générer une multitude de serials valides.

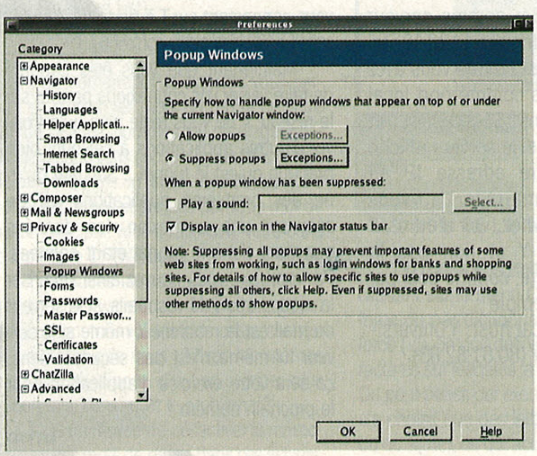
La référence en matière de recherche de cracks reste http://astalavista.box.sk

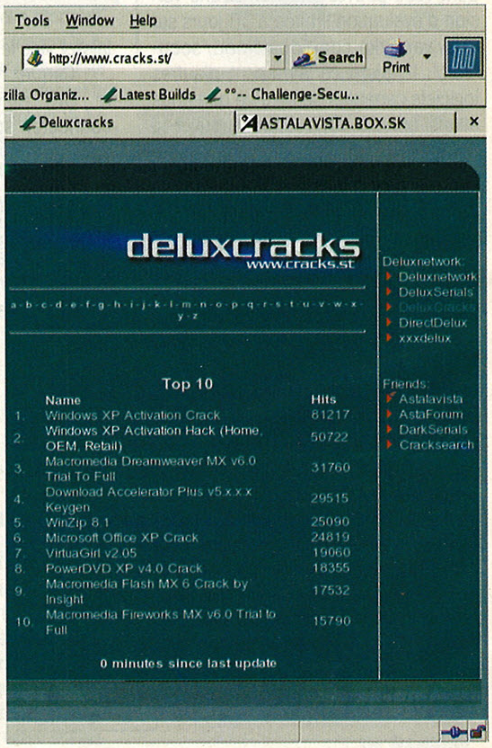
Ce site ne propose pas de cracks, mais uniquement un moteur qui référence les meilleurs sites. Sa qualité a fait sa réputation. À ne pas confondre avec astalavista.com ou astalavista.net ! On peut rechercher par exemple les mots-clé " Winzip 8.1 " et le moteur renverra une liste de bons sites possédant un crack pour ce logiciel.

Parmi les meilleurs sites proposant des cracks en téléchargement, notre choix s'est porté sur http://www.cracks.st (voir photo d'écran).

Pour les sérials, son partenaire http://www.deluxserials.com est également de bonne qualité. Un autre site intéressant : http://www.darkserials.com.

Utilisez les liens partenaires si vous ne trouvez pas votre bonheur sur ces sites. Une recherche sur google peut également donner des resultats, mais ils sont souvent brouillés et rarement plus efficaces que sur astalavista.





ANONYME OU FLIQUÉ ?

Plutôt fliqué, hélas. Mais un lecteur de Pirat'z averti en vaut deux ! Armé de notre précieux dossier sur l'anonymat du numéro précédent, vous ne devriez pas avoir de problèmes à rester discret malgré les dispositifs de surveillance mis en place.

La majorité des sites de cracks conservent des logs. Ceux-ci contiennent l'adresse IP des ordinateurs qui se connectent au service, ainsi que les requêtes qu'ils ont faites et les fichiers qu'ils ont téléchargé.

Ces informations sont-elles transmises ou interceptées par des services de police ? On peut le supposer, mais jusqu'à présent ces services ont toujours cherché à s'attaquer aux "gros poissons" (revendeurs de logiciels piratés, responsables de sites ftp warez) plutôt qu'aux utilisateurs finaux. Ouf. Jusqu'au jour où les éditeurs de logiciels suivront la piste des majors de la musique en Amérique, où depuis cet été les utilisateurs du célèbre logiciel de Peer 2 peer Kazaa sont traqués et traînés devant les tribunaux.

Heureusement, on n'en est pas là, et télécharger un crack sur Internet reste relativement anodin. Les risques sont faibles dans tous les cas, et sont même nuls si vous avez bien acheté la version originale du logiciel que vous souhaitez cracker. Par contre, ces logs sont parfois accessibles à tous les utilisateurs du site, comme le prouve la photo d'écran ci-contre. Celle-ci montre les 10 dernières recherches de cracks effectuées sur le site, avec l'adresse IP des internautes correspondants !

Si vous n'avez pas pris la précaution de passer par un proxy, n'importe qui pourrait ainsi savoir que vous venez de télécharger un crack... Retrouver votre nom à partir de l'adresse IP est simple pour les forces de l'ordre, mais pas pour un particulier. Pourtant, mieux vaut se méfier, car sur un petit nombre de fournisseurs d'accès (comme Nerim pour ne pas le citer), une astuce faisant intervenir leur serveur de mail peut permettre de retrouver votre vrai nom en connaissant simplement l'adresse IP ! OOooops.

METTRE DES CRACKS SUR SON SITE PERSO

Certains sites proposent des bouts de code HTML à insérer sur une page de son site web. Ainsi, vous pourrez proposer à vos visiteurs un moteur de recherche de cracks ou de serials, sans vous fatiguer à mettre à jour vous-même une telle base de données !

Sachez cependant que la légalité de la chose n'est pas très claire. A notre connaissance, il n'existe pas de jurisprudence ayant déclaré que la mise en ligne de cracks est illégale, cependant, cela pourrait évoluer. Tout va dépendre de la mise en place ou non de la loi sur la confiance dans l'économie numérique, prévue pour... le premier janvier 2003 (et oui, mêmes les sénateurs peuvent être en retard).

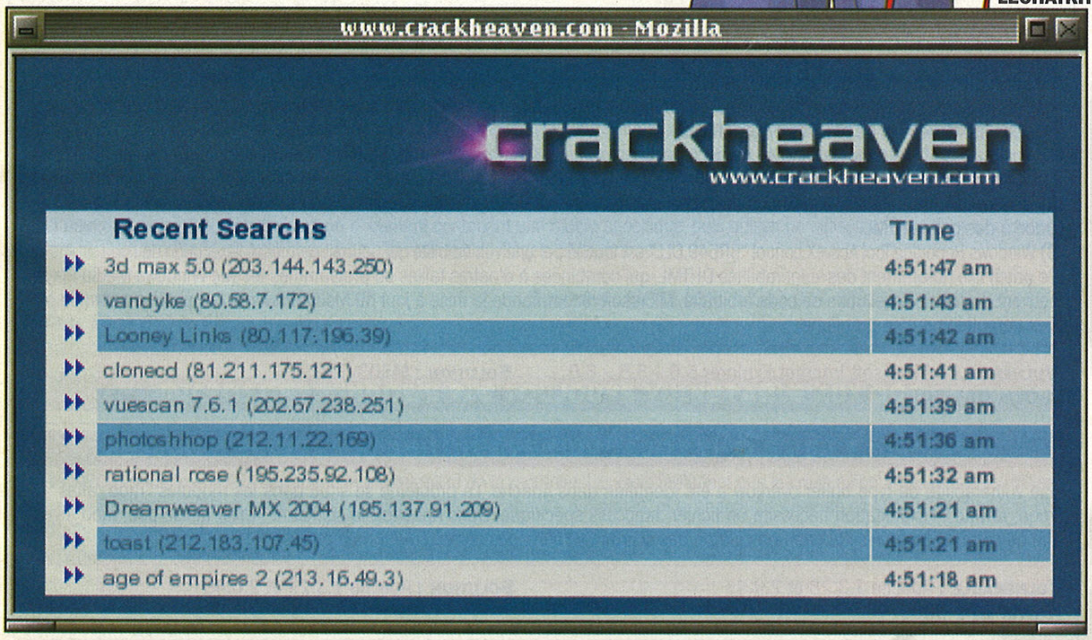
Voici un code qui permettra à vos visiteurs de rechercher des serials à partir de votre site , en utilisant le service proposé par crackheaven.com :

```
<form
action="http://www.crackheaven.com
/search.php" method="POST">
<INPUT TYPE='hidden' name='Powe-
redBy' value='nom_de_votre_site'>
<INPUT TYPE='hidden'
name='PoweredBy_URL'
value='http://www.votre_site.com'>
<input size="40" name="str">
<input type="submit" value="search">
</form>
```

Il vous suffit d'insérer ces lignes quelque part sur une page de votre site web, et le tour est joué.

BONNE CHASSE !

LECHATKITU



IZ

DERNIÈRES VOLONTÉS PAR E-MAIL.

Un nouveau service Web propose aux internautes l'expédition par mail de leurs derniers messages après leur mort ! Ce service morbide mais innovant permet la sauvegarde de messages qui seront ensuite envoyés aux personnes désignées après la mort du propriétaire du compte. Pour sa promotion, ce site rappelle que la mort peut survenir à tout moment et qu'il faut donc se dépêcher de souscrire. Le prix ? 9,99 dollars (un peu moins en euros) tous les trois ans.

COPIE PRIVÉE : LOI DE FIN DE RÈGNE POUR LE CD

En même temps qu'il autorise le verrouillage des CD, le nouveau texte de loi du gouvernement français conserve le principe de la copie privée. C'est dire si ce texte, qui contient en lui-même sa propre contradiction, est mauvais ! Concrètement, et pour éviter les inévitables cafouillages, la nouvelle loi instaure un collège de " médiateurs ". Il s'agira de fonctionnaires ou de magistrats, dont on nous promet qu'ils seront indépendants, et qui seront chargés de trancher les litiges. Ils décideront ainsi, au cas par cas, de ce qui relève de la copie privée ou de la contrefaçon... On voit bien que cette loi, pas encore votée heureusement, ressemble à un acte désespéré des majors aux abois pour tenter défendre un support mourant, trop cher et élaboré au siècle dernier : le cd. La nouvelle loi prévoit aussi un dépôt légal pour les pages internet des sites web. Comme les journaux et les livres, celles-ci devront être échantillonnées et archivées par l'administration, qui n'a visiblement pas de problème plus urgent à régler. Transmis au Parlement, ce texte pourrait être voté au cours du premier semestre 2004.

VULNERABILITES

SEPTEMBRE, OCTOBRE, NOVEMBRE, 2003

WOOHOO, LES ROMS SONT LÉGALES!

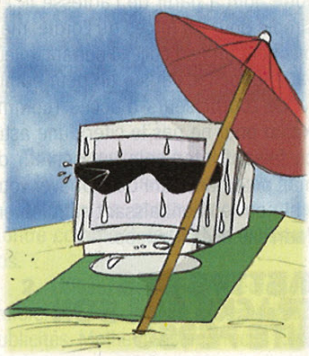
Euh, en fait, non. C'est pourtant ce qu'ont cru (ou voulu) comprendre de nombreux internautes fans d'émulation, qui ont mal interprété une modification récente du DMCA américain. Rappelons que le DMCA interdit en particulier l'utilisation - comme la distribution - de toute technologie visant à contourner une protection contre la copie. Conséquence : les créateurs d'émulateurs ou de solutions de copie pour les vieux jeux de systèmes maintenant dépassés se retrouvaient dans l'illégalité. Cette interdiction vient d'être levée aux USA pour les systèmes obsolètes, ce qui a déclenché une vague d'enthousiasme un peu trop fébrile dans le monde de l'émulation. Les lois sur le droit d'auteur ne sont pas changées, ce qui signifie qu'il est toujours illégal de télécharger des ROMs sur le net (sauf sur www.pdroms.de bien entendu), de les mettre sur votre site web ou dans votre partage eDonkey. Par contre, si vous êtes américain et que vous avez un dispositif pour copier vos cartouches NES sur votre ordinateur, vous pouvez l'utiliser librement. Rassuré?

RIAA = PIRATE

Sharman Networks porte plainte contre la RIAA qui a utilisé un logiciel piraté, oui oui!, rien de moins que Kazaa Lite, pour surveiller les utilisateurs et accumuler des renseignements personnels sur eux. C'est donc la RIAA qui se fait attaquer pour avoir enfreint les lois sur le droit d'auteur! Et grâce à leurs changements dans la licence d'utilisation, Sharman Networks peut dire que même si la RIAA avait utilisé le logiciel original, elle aurait également été en infraction. Prochaine étape, une loi interdisant d'interdire le piratage?

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

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



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

PAR : CHAOUKI BEKRAR AKA REYNO
EN COLLABORATION AVEC L'EQUIPE TECHNIQUE DE www.K-OTik.com

INTERNET EXPLORER FILE DOWNLOAD & EXECUTION VULNERABILITY

Plusieurs nouvelles vulnérabilités critiques (ou variantes de failles connues) on été identifiées dans Microsoft Internet Explorer. Ces problèmes pourraient permettre le téléchargement et l'exécution d'un Trojan/Virus via une simple page HTML.
1) La première vulnérabilité "Double slash zone transfer" peut être exploitée grâce au double slash ":\\" dans la location CODEBASE, ce qui permettra de passer outre les critères de sécurité définis par IE et donc accéder aux ressources locales.
2) Le second problème "Userprofile disclosure", permet d'accéder aux fichiers de l'utilisateur actuel sans connaître son login (en remplaçant ce dernier par "file:///::{450D8FBA-AD25-11D0-98A8-0800361B1103}"), il est possible de voir le profil de l'utilisateur actuel via le script "alert(window.open("file:///::{450D8FBA-AD25-11D0-98A8-0800361B1103}/res::"))"
3) Le troisième problème "Redirection and Refresh in IFRAME parses local file" peut être exploité afin d'afficher des fichiers locaux grace à une IFRAME dont le SRC pointe vers une ressource distante qui redirige vers une ressource locale (avec une Actualisation automatique de la page).
* Un Test de Sécurité (Online) est disponible à l'adresse :
http://www.k-otik.com/news/11.08.Exploits.IE.php

VULNÉRABLE : Microsoft Internet Explorer 5.0 - 5.5 - 6.0 **SOLUTION :** Désactivez Active-Scripting
K-OTIK ID : Not Assigned

MIRC 6.12 UNSPECIFIED DCC REQUEST VULNERABILITY

Une vulnérabilité de type Déni de Service a été identifiée dans mIRC. Cette faille est causée par des erreurs dans les requêtes DCC, qui peuvent être exploitées afin de crasher le client d'un utilisateur.
(Exploit) mIRC alias:

```
/crash { .raw PRIVMSG $1 $+(:,$chr(1),DCC) send " $+ $str($rand(a,z) $+ $chr(32),250) $+ " 0 2130706433 $+(8192,$chr(1)) }
```

Une nouvelle variante de l'exploit a été identifiée, elle pourrait être exploitée afin de causer un Déni de Service. Le problème se situe dans l'option DCC qui ne manipule pas correctement les longs noms de fichiers (exploitation possible seulement si la fenêtre de transfert est minimisée).

VULNÉRABLE : mIRC 6.12 **SOLUTION :** Utiliser "/ignore -d *" ou "/ignore -wd *"
K-OTIK ID : 0381

MICROSOFT INTERNET EXPLORER OBJECT DATA VULNERABILITY

L'équipe de Microsoft vient de publier un patch cumulatif qui fixe plusieurs vulnérabilités critiques (variantes de la faille MS03-032) présentes dans Internet Explorer. La vulnérabilité Object Data peut permettre à un attaquant distant l'exécution de commandes arbitraires via de simples pages HTML.
1) Vulnérabilité impliquant le modèle de sécurité cross-domain d'Internet Explorer. Ce problème a pour conséquence l'exécution de scripts arbitraires via des pages HTML.
2) Internet Explorer ne détermine pas correctement les types d'objets, ce qui pourrait permettre l'exécution de code arbitraire grâce à des pages HTML.
3) Windows Reporting Tool ActiveX control "BR549.DLL" est touché par une vulnérabilité qui pourrait permettre l'exécution de code arbitraire. Ce patch fixe notamment des vulnérabilités DHTML, qui combinées à d'autres failles ou programmes tel que Windows Media Player, peuvent permettre l'exécution de code arbitraire. Microsoft recommande la mise à jour du Media Player car ce patch ne semble pas fixer complètement ce problème.

VULNÉRABLE : Microsoft Internet Explorer 5.0 - 5.5 - 6.0 **SOLUTION :** MS03-040
K-OTIK ID : 0368

APACHE 1.3.28 / 2.0.47 LOCAL VULNERABILITIES IN VARIOUS MODULES

Une vulnérabilité de type buffer overflow a été identifiée dans Apache. Le problème se situe dans les modules "mod_alias" et "mod_rewrite", l'exploitation nécessite un fichier .htaccess spécifique. Dans Apache2 le socket AF_UNIX utilisé par "mod_cgid" afin de communiquer avec le daemon cgid ou des scripts CGI n'est pas correctement manipulé.

VULNÉRABLE : Apache 1.3.28 et 2.0.47 **SOLUTION :** Apache 1.3.29 et 2.0.48
K-OTIK ID : 0407

WINAMP 2.91 IN_MIDI.DLL ARBITRARY CODE EXECUTION

Winamp souffre d'une vulnérabilité qui pourrait permettre l'exécution d'un code arbitraire via des fichiers MIDI. Le problème se situe dans le plugin IN_MIDI.DLL utilisé pour l'exécution de fichiers MIDI, en remplaçant la valeur "Track data size" d'un fichier MIDI par la valeur 0xffffffff, on observe ce qui suit :

```
4 bytes MIDI Header   "MThd"
4 bytes Header data size 00000006
2 bytes Format      0000
2 bytes Number of tracks 0001
2 bytes Divisions     0001
4 bytes Track Header   "MTrk"
4 bytes Track data size  ffffffff <--- bug
...  "aaaaaaaaaaaaaaaaaaaaa..."
```

VULNÉRABLE : Winamp 2.91 **SOLUTION :** Winamp 3.00
K-OTIK ID : 0336

YAHOO! MESSENGER FILE TRANSFER DENIAL OF SERVICE

Une vulnérabilité de type Déni de Service a été identifiée dans Yahoo! Messenger. Cette faille résulte d'une erreur dans le fonction de transfert "ft.dll", ce qui pourrait être exploité en envoyant une requête spécifique de transfert de fichiers, qui provoquera le crash du client (Si la victime accepte le transfert de fichiers).

```
YMSGR:sendfile?[Victim_yahooID]+%%%&c%c:\[fichier]
```

VULNÉRABLE : Yahoo! Messenger version 5.6 **SOLUTION :** Ne pas accepter le transfert de fichiers.
K-OTIK ID : 0400

AOL INSTANT MESSENGER FILE TRANSFER ERROR MESSAGE OVERFLOW

Une vulnérabilité de type buffer overflow a été identifiée dans AIM. Ce problème est causé par une erreur dans la fonction "CCertsByUserName::Cleanup()" qui se situe dans "AimSecondarySvcs.dll", la fonction "sprintf()" est utilisée de manière non sécurisée pendant la construction d'un message d'erreur (problème de connexion avec un utilisateur). Cette faille pourrait être exploitée via le protocole "aim:" qui ne gère pas correctement les opérations "getfile" suivies d'un paramètre "screenname" relativement long.

```
aim:getfile?screenname=AAA...[x1130]...AAA
```

VULNÉRABLE : AIM version 5.2.3292 Windows **SOLUTION :** AIM version 5.5.3415 Beta
K-OTIK ID : 0388

MICROSOFT ACCESS SNAPSHOT - VB - WORDPERFECT - WORD/WORKS

MS03-038 : Une vulnérabilité a été identifiée dans le contrôleur ActiveX de Microsoft Access Snapshot Viewer, elle pourrait causer un buffer overflow via des documents HTML ou des fichiers Microsoft Access Snapshot. Le problème est que Microsoft Access Snapshot Viewer ne vérifie pas correctement certains paramètres, ce qui pourrait être exploité en créant un fichier spécifique Access Snapshot, qui permettra l'exécution d'un code arbitraire avec les privilèges de la victime.
MS03-037 : Une vulnérabilité a été identifiée dans Microsoft Visual Basic for Applications (VBA), elle pourrait permettre à des documents HTML de causer un buffer overflow. Le problème est que VBA ne vérifie pas correctement certaines propriétés avant de traiter un document, ce qui pourrait permettre à un attaquant malveillant de créer un fichier (Word ou Excel par exemple), qui causera un buffer overflow dès l'ouverture du document par un utilisateur.
MS03-036 : Une vulnérabilité a été identifiée dans le convertisseur WordPerfect de Microsoft Office, elle pourrait permettre l'exécution de code arbitraire sur un système vulnérable. Le problème est que certains paramètres ne sont pas correctement vérifiés avant le processus de conversion, ce qui pourrait provoquer (via des documents malveillants) un débordement de tampon, et donc l'exécution d'un code arbitraire. La vulnérabilité se situe dans la conversion des documents Corel WordPerfect.
MS03-035 : Une vulnérabilité a été identifiée dans Microsoft Word et Works Suite, qui pourrait être exploitée par des attaquants distants afin d'exécuter du code arbitraire sur un système cible. Une macro est une série de commandes et d'instructions qui peuvent être groupées en une seule et simple commande afin d'exécuter une tâche automatiquement. La vulnérabilité est causée en raison d'une erreur dans la vérification des propriétés des documents modifiés, permettant ainsi de contourner le model de sécurité configuré par l'utilisateur.
Ceci peut être exploité en construisant un document contenant une macro spécifique, puis obliger un utilisateur à ouvrir ce document, ce qui provoquera l'exécution du code arbitraire avec les privilèges de la victime.

VULNÉRABLE : Microsoft Office 2000 – XP **SOLUTION :** MS03-038 - MS03-037- MS03-036- MS03-035
K-OTIK ID : 0327

MICROSOFT WINDOWS RPC TOUJOURS VULNÉRABLE AUX DOS

Une nouvelle vulnérabilité de type Déni de Service a été identifiée dans Windows malgré le patch MS03-039 . Cette faille est causée par une race condition provoquée par certaines requêtes RPC (résultat de l'utilisation de deux fils pour manipuler la même requête RPC), ce qui mène à la corruption et à l'instabilité de la mémoire. Les tests indiquent que le crash a lieu après plusieurs milliers de requêtes. Les conditions telles que la vitesse du CPU, la capacité du réseau, et la charge du système cible sont des facteurs importants. L'équipe de K-OTik n'a pas démontré que cette vulnérabilité peut être exploitée afin d'exécuter des commandes arbitraires, cependant la vulnérabilité de Windows 2003 Server a été prouvée.

VULNÉRABLE : Windows 2000 – NT – XP - 2003-11-11 **SOLUTION :** Bloquer les ports 135, 137, 138, 445
K-OTIK ID : 0380

UN NOUVEL ACE ?

COCO a volé le nom de ACE pour son nouveau groupe, Actual Cracker Entertainment. Il a fondé ce groupe avec d'anciens ennemis (THE MAGIC CIRCLE).
TPI, de BEASTIE BOYS, aurait également rejoint ACE, avec deux ex-membres de MCL. Mais les nouvelles d'aujourd'hui disent qu'ils auraient laissé tombé ACE, ne pouvant supporter que COCO vole des routines de TCS pour ses intro. TPI veut fonder un nouveau groupe avec THE DARKNESS et ALPHAFIGHT. Le groupe s'apellera probablement MASK !
Sinon, plusieurs membres de NEW EDITION ont lâché le groupe pour créer HIGH-TECH BOYS.

MAMIE FAIT DU P2P

Les méthodes d'intimidation de la RIAA, pour dissuader les utilisateurs de peer2peer, se veulent impressionantes. Récemment, plus de 200 internautes américains recevaient un courrier les informant de poursuites judiciaires, pour avoir partagé de la musique sous copyright. Parmi ces personnes, une américaine partageait sur KaZaa plus de 2000 MP3, dont un bon nombre de morceaux de Hip-Hop " appartenant " au majors à l'origine de ces actions. Bon, l'américaine en question, elle a 66 ans. Bien sûr son âge ne doit pas l'empêcher d'écouter ce genre de musique. Mais elle est sans doute aussi très douée en informatique, vu qu'elle arrive à utiliser KaZaa sur son vieux Apple Macintosh, alors que ce réseau de p2p n'est prévu que pour Windows...
Bref, encore une preuve que la lutte contre le piratage n'est pas si efficace que ça et qu'elle n'est pas sans risque pour les libertés individuelles et la protection de la vie privée. Attention, en France aussi, les FAI peuvent être appelés à collaborer avec les maisons de disques.

LA SCENE PIRATE

Nous vous parlions, dans le dernier numéro, de la fin controversée de Fairlight, un groupe mythique de la scène d'autrefois. Dans ce dossier nous désirons revenir sur l'age d'or des pirates et vous faire comprendre comment la scène fonctionnait il y a vingt ans, bien avant la généralisation du Net, alors qu'on pouvait déjà se procurer facilement des milliers de jeux pour son ordinateur 8bits.

LA RIAA FAIT RIRE D'ELLE AU SÉNAT

Un sénateur américain demande l'arrêt des amendes excessives contre les utilisateurs de P2P. En effet, le sénateur Norm Coleman déclare que les amendes de 750 à 150 000$ par chanson téléchargée sont exagérées (sans blague). Selon le sénateur, cela forcerait les gens à régler à l'amiable plutôt que de défendre leur cause en cour, surtout lorsque le montant réclamé se chiffre à des millions de dollars. Coleman a remis en doute les tactiques de la RIAA depuis un certain temps en observant les outrageuses poursuites intentées par ces derniers. Par exemple, un adolescent de 12 ans qui se retrouve avec des poursuites de plusieurs millions sur les bras, ou cette pauvre femme de 66 ans qui a été poursuivie pour une somme de 300 millions de dollars. Pour éviter ce genre de "gaffe", le sénateur désire qu'un juge approuve les subpoenas et que l'on s'assure de l'identité de la personne avant de lancer des poursuites idiotes contre des innocents comme dans les deux cas exposés plus haut. Ouf, il n'y a donc pas que Pirat'z qui trouve la RIAA bien ridicule.

DU NOUVEAU EN ALLEMAGNE

Il semble que RAW DEAL revienne sur la scène du 64, avec un crack de Battle Ships. En même temps, un nouveau groupe s'est formé en Allemagne : THE WANDERER GROUP. Avec SPEEDCRACKER (ex-TRIANON) et STARLINE. Faites attention avec leur cracks, ils promettent de ne faire que "Reisende im Wind 2", "Schatzjaege" et d'autres atrocités allemandes.

Soyez aussi prudents avec les cracks de THE FANTASTIC CREW. Ce sont les pire en***** de recrackers de la planète. Ils ont repris le crack de Battle Ships par LAFFEN (RDI), mais ces imbéciles ont oublié d'enlever le message "SMASHED BY LAFFEN".

Savez vous quel est l'ordinateur le plus vendu au monde ? C'est le Commodore 64, avec au moins 20 millions d'unités vendues depuis 1982. Le 64 dans le nom, c'est pour 64 K de RAM (oui, des kilooctets, pas des mégas !); vous vous doutez que ce n'est pas la machine la plus puissante jamais fabriquée. Pourtant, c'était en quelque sorte la console de jeu des années 80, puisqu'on pouvait l'acheter à un prix très raisonnable, sous la forme d'un petit clavier à brancher sur son téléviseur. Avec ce succès, des milliers et des milliers de jeux ont été développés pour cette plate forme.

À cette époque, les PC compatibles d'IBM (8086) existent déjà, mais ne séduisent pas encore le grand public. Les ordinateurs d'Atari, de Sinclair ou d'Amstrad ont leurs fans, mais ne connaissent pas un engouement aussi général que le Commodore. Nous allons donc surtout nous intéresser au C64, parce qu'il est le symbole de cette époque. C'est l'ordinateur qui s'est imposé durablement comme la machine favorite des joueurs et, c'est ce qui nous intéresse ici, des pirates de jeux vidéo !

LES JEUX

Les jeux d'il y a vingt ans n'ont pas grand chose à voir avec ce qui se fait actuellement. Il faudrait plutôt les comparer à certains jeux en flash, ou ceux de vos téléphones portables : un principe simple, avec des niveaux et une difficulté croissante. La plupart des jeux étaient réalisés en 2D, avec des animations et des moyens graphiques limités par la machine. Mais il y avait beaucoup d'exceptions à ces règles et des titres vraiment géniaux ont été conçus pour cet ordinateur. C'était les concepts, plus que la réalisation graphique ou l'effet d'immersion, qui faisaient le succès des jeux.

Il y avait des jeux d'arcade, surtout, avec de l'action simple, un personnage à contrôler et des ennemis. Il y avait pas mal de jeux de rôle aussi, dont beaucoup n'avaient qu'une interface textuelle – pour les puristes. Une des catégories les plus appréciées était encore la simulation de sport. Et puis il y avait tous ces jeux inclassables, bizarres ou incompréhensibles, qui faisaient (et font encore !) le charme de cette machine.

La taille de ces jeux variait entre quelques kilobytes et plusieurs disquettes (environ 176K par face). Bien qu'ils étaient vendus séparément, on pouvait souvent en faire tenir une série sur une seule disquette. Certains éditeurs, peut-être pour concurrencer les compilations pirates, vendaient aussi des collections de plusieurs jeux.

LES PROTECTIONS

Il existait des programmes plus ou moins efficaces pour copier les jeux originaux. Certaines protections ne résistaient pas à la copie bit à bit de la disquette. Des programmes spécialisés pouvaient quelque fois tromper les mécanismes de protection.

LA COMPILATION D'UTILITAIRES FAST HACK'EM

Mais la majorité des jeux ne pouvait pas être copiée si facilement. Certains éditeurs utilisaient la protection par code : on devait entrer des mots du manuel (ou d'une grille codes difficile à photocopier) pour pouvoir jouer. D'autres types de protection utilisaient des disquettes modifiées, ou des secteurs spéciaux, pour marquer les originaux. Plus rares, il y avait encore les dongles, des petits dispositifs à brancher sur un port de l'ordinateur.
Dans tous ces cas, le travail des crackers était le même : identifier toutes les routines de vérification et les supprimer. La première difficulté consistait à passer les techniques spéciales de chargement du jeu pour accéder au vrai programme. Ensuite, il fallait y supprimer toutes les vérifications – et les éventuelles contre-vérifications. Quelques protections compliquées déclenchaient des vérifications au milieu du jeu, aléatoirement. Il fallait donc tester entièrement le jeu pour être sûr qu'il était bien cracké.
Notez que ces méthodes de protections sont encore d'actualité – ainsi que les méthodes pour les cracker.

LES GROUPES

Il est difficile de dire qui a cracké les premiers jeux sur C64, parce que c'étaient des individus isolés qui ne cherchaient pas tellement à distribuer leurs copies. Mais rapidement les pirates se sont organisés en groupes, surtout avec le C64 : une culture underground s'est créée, avec ses règles tacites, ses héros et ses querelles.

L'atout le plus important de la scène était d'avoir des contacts. On cherchait à avoir le plus possible de jeux et l'échange était le moyen le plus efficace et le plus économique de s'en procurer. Les groupes se formaient entre ces personnes en contact, pour mieux se répartir les tâches.

SE PROCURER LES ORIGINAUX

Pour cracker un jeu, il fallait bien entendu en obtenir la version originale. Chaque groupe avait ses sources pour obtenir ces versions le plus tôt possible. Certains profitaient de fuites chez les éditeurs, et avaient des contacts qui pouvaient leur envoyer les jeux avant leur commercialisation. D'au-

DES ANNEES 80

tres avaient des contacts dans la presse et profitaient des versions de démonstration, parfois incomplètes (previews). On pouvait aussi se faire envoyer les jeux de l'étranger, quand ils y sortaient plus tôt en magasin (l'Angleterre, notamment, était la première servie en Europe).

Les crackers

Les vraies stars de la scène étaient naturellement les crackers, les plus doués, qui étaient capables de faire sauter les protections des jeux. C'étaient en général des jeunes hommes de 16 à 25 ans, passionnés par leur machine, mais paradoxalement peu intéressés par les jeux qu'ils piratait. Un bon cracker pouvait s'occuper de dizaines de jeux en un mois.

C'était aussi eux qui programmaient les intros qu'ils insèraient au début du jeu. Voir l'encadré sur les démos et les intros.

Les swappers

Une fois qu'un jeu avait été correctement cracké et habillé d'une intro aux couleurs du groupe, il s'agissait de le distribuer le plus rapidement possible : c'était une question de prestige. En général, les nouveaux membres recrutés par les groupes étaient employés à cette tâche. Il fallait réaliser des copies en masse et les faire parvenir à tous ses contacts.

Les pirates utilisaient généralement des boites postales, afin de préserver un minimum leur anonymat. Comme la poste internationale coûtait cher, ils utilisaient des faux timbres, ou des colles spéciales qui leur permettaient de les réutiliser plusieurs fois. Lorsque les employés de la poste s'en rendaient compte, il ne fallait pas s'étonner d'avoir à faire à la police en relevant le courrier.

A la fin des années 80, les premiers modems ont commencé à apparaître (voir l'encadré sur les télé conférences) et les échanges se firent plutôt par BBS. Mais ça c'est une autre histoire.

Les motivations

On peut penser que les pirates distribuaient leurs jeux pour se faire de l'argent. Pourtant, ils ne demandaient en général qu'un minimum, afin de rentrer dans leur frais, parce que la poste et l'investissement dans les originaux coûtaient cher. Il est vrai, cependant, que des gens tentaient ouvertement de s'enrichir en vendant des jeux piratés par correspondance, à petite ou à large échelle. Ce commerce n'étaient cependant pas si profitable, parce qu'ils avaient toutes les chances que la police s'intéresse à eux. C'étaient les premiers à tomber, presque sans exception. Et c'est toujours vrai.

La raison qui poussait les pirates à copier des jeux tenait plutôt d'un désir de liberté. Les jeux étaient déjà chers à l'époque, et ils estimaient que les jeunes et les moins fortunés devaient avoir la possibilité d'utiliser les jeux et les programmes qu'ils crackaient. De plus les crackers étaient frustrés de ne pas pouvoir copier librement à des amis les programmes qu'ils avaient trouvés, ou de pouvoir observer comment ils fonctionnaient, à cause des protections. Les pirates disaient lutter pour la libre circulation de l'information.

(Une réponse plus intelligente à ce problème a, à mon avis, été donnée, dans une autre contexte culturel, par le logiciel libre : http://www.gnu.org ou http://www.framasoft.net/.)

LES TÉLÉ-CONFÉRENCES

Les pirates communiquent aujourd'hui par l'Internet et l'IRC. À l'époque, les utilisateurs du Net n'étaient pourtant que des privilégiés. Les pirates, dont les contacts pouvaient s'étendre sur plusieurs continents, avaient tout de même les moyens de se contacter : par téléphone.

Ils usaient bien sûr de modems (quand ils pouvaient s'en procurer un), pour s'échanger les copies de jeux. Mais ils dialoguaient abondamment par télé-conférence. Certains opérateurs fournissaient en effet des services qui permettaient à un groupe de personnes de parler ensemble, par téléphone. Il n'était pas rare de recevoir un coup de fil au milieu de la nuit, pour vous demander si vous ne vouliez vous joindre à une conférence, à l'autre bout de la planète.

Évidemment, ce genre de service, surtout d'un pays à l'autre, n'était pas donné. Mais la plupart avaient fait leur spécialité du piratage des lignes téléphoniques (phreaking), et ne déboursaient pas un sous pour ces communications, payées par les opérateurs ou des entreprises malchanceuses.

A une époque, AT&T, et d'autres opérateurs américains, ont mené une vrai chasse aux pirates, en traquant les communications suspectes vers l'Europe et en essayant de piéger les petits malins. Les télé-conférences ont cessé petit à petit parce qu'elle étaient trop dangereuses, marquant la fin d'un âge d'or. Mais c'était bientôt le début du nouvelle ère, celle d'Internet.

Le phreaking existe toujours au 21e siècle. La téléphonie mobile et numérique offre cependant autant de nouvelles perspectives que de difficultés et de risques supplémentaires.

ÊTRE ARRÊTÉ, À L'ÉPOQUE

A part aux États-Unis peut-être, les polices spécialisées dans le piratage et la criminalité informatique n'existe réellement que depuis peu de temps. C'était une police traditionnelle qui s'occupait des problème de piratage. On dit d'ailleurs que les pirates ne craignaient les perquisitions qu'aux heures de bureau : lorsqu'ils sentaient que quelque chose allait arriver, il cachaient leur matériel la journée et se sentaient en sécurité le soir et les week-ends, pour vaquer à leurs occupations illégales.

Lorsque la police parvenait à arrêter le membre d'un groupe, elle tentaient de négocier avec lui, pour qu'il donne ses contacts (ça existe encore). Lorsqu'on apprenait qu'un puis deux membres étaient tombés, les temps devenaient difficiles et c'était le moment de faire profil bas. Pourtant, les personnes qui risquaient le plus étaient celles qui vendaient les copies pirates. Le fait, proprement dit, de cracker les originaux n'était pas condamnable à moins d'avoir la preuve que les copies étaient distribuée. Les lois, de ce côté, tende à notre époque à devenir plus préventive et plus restrictive, au point d'interdire, selon les pays, de fabriquer, de posséder ou de distribuer des outils qui peuvent servir à cracker des logiciels.

'Z

Virus et Spam, même combat

Dans ma boîte aux lettres, je reçois presque autant de virus et de spams que d'invitations à dîner de la part de blondes à forte poitrine, c'est tout dire. Eh bien, pas étonnant, car parmi les créateurs de virus, on retrouve... les spammeurs! Ceux-ci, toujours à l'affut de nouveaux moyens d'envoyer leurs emails en masse et de récupérer de nouvelles adresses, seraient en effet à l'origine de virus comme Mimail, capable de collecter les adresses qu'il trouve, d'envoyer des emails, et même de lancer une attaque DOS contre des sites anti-spam!

Cours d'autodéfense

Une nouvelle organisation, Subpoena Defense Alliance, a été mise sur pied afin de donner des conseils aux utilisateurs de logiciels P2P afin qu'ils évitent les poursuites. De plus, s'ils sont déjà dans la ligne de mire de la RIAA cette organisation leur donnera des trucs par rapport à leur défense. Il leur est ainsi conseillé de ramener la faute sur leur grand-mère de 66 ans, leur fils de 12 ans, le virus qu'a ramené Henri de l'internet, le pape Jean-Paul II, ou encore Pirat'z. Euh, finalement, évitez Pirat'z, on se passera de la publicité gratuite.

Allez, au boulot!

L'Université de Floride a créé un outil permettant de dégager le réseau des logiciels P2P. Ce nouveau logiciel, baptisé Icarus, est apparemment un véritable succès. Il a été déployé au début de l'été sur le réseau du campus. Ce sont les programmeurs de l'école qui ont développé le programme open-source afin d'enrayer le partage de fichiers parmi les étudiants. Les représentants du campus déclarent que 90% du trafic internet, avant l'implantation du programme, était dû au partage de fichiers. Les 10% restant, c'était quoi, du trafic FTP?

LA COMPÉTITION

Le moteur le plus stimulant de la scène était sans aucun doute la rivalité qui régnait entre les clans. Les groupes essayaient par tous les moyens d'être les premiers à sortir la version pirate des nouveautés. Ils cherchaient à impressionner la communauté pour gagner respect et reconnaissance.

Cette compétition se retrouvait aussi fortement dans la réalisation des intros, et plus encore dans les démos. On voulait toujours faire plus fort et plus rapide que les autres. C'est cette interaction qui a poussé les programmeurs à dépasser les limites de la machine et à inventer toujours de nouvelles subtilités pour contourner les difficultés techniques. Ironiquement, beaucoup des techniques développées pour les démos ont inspiré les éditeurs de jeux (lorsqu'ils n'engageaient pas les crackers eux-mêmes).

TRIAD

TRIAD est une figure emblématique de la scène. C'est l'un des quelques groupes encore en activité, et ce fut l'un des plus grands, des plus productifs et des plus reconnus de son époque. Ils ont d'ailleurs influencé la scène avec une série d'idée novatrices, comme le cheat modus (voire encadré) ou leurs intros avec un code de couleur pour donner leur jugement sur le jeu.

TRIAD a été fondé en Suède le 28 juillet 1986, à 21h30, par Arrow, Fred, Skydive, Ixion, Lucifer, RND et Mr. Z. En 86, Arrow et Fred de CoD faisaient de nombreux échanges de jeux pirates avec des contacts partout dans le monde (ils recevaient 4 ou 5 courriers par jour). En rencontrant Ixion de 3001, ils se sont en plus assurés un accès régulier aux nouveautés (originaux), et les deux groupes ont commencé à collaborer intensément. Rapidement, un contact de 3001, Mr. Z, et son vieil ami RND se sont joints à eux pour former une triade qui représentait les trois talents de la scène : obtenir les originaux, les cracker et les distribuer.

Jusqu'en 1993, en Suède, les échanges personnels de jeux copiés étaient parfaitement légaux. Ainsi, les groupes pouvaient évoluer librement, tant qu'ils ne vendaient pas leurs versions. TRIAD avait d'ailleurs un contact dans une société d'importation de

LES TRAINERS : CES PETITS PLUS DES VERSIONS PIRATES

Pour vérifier que les jeux étaient entièrement crackés, les pirates consciencieux en testaient tous les niveaux, jusqu'à la fin. Évidemment, les jeux étaient en général plus linéaires et moins complexes que maintenant. Pourtant ils n'étaient pas tous des champions du jeu vidéo et finir certains jeux n'était pas sans demander de l'acharnement et un long entraînement.

Pour supprimer les protections, les crackers devaient avoir une connaissance assez intime des jeux. Ainsi, ils remarquaient au passage les parties du programme qui décrémentaient le nombre de vies restantes ou diminuaient les niveaux d'énergie. A côté de certaines protections, c'était un enfantillage pour eux de faire sauter ces conditions et rendre les personnages immortels.

Ce sont des membres de TRIAD, Ixion et Mr. Z, qui ont eu la première fois l'idée de donner cette possibilité aux joueurs. Ils suffisaient d'appuyer sur C ou T (pour cheat et trainer), durant l'intro du jeu, pour accéder à un menu de triche. C'était le premier groupe à le faire, et leur idée a été reprise jusqu'à nos jours.

LE CHEAT MODUS DE BANGKOK KNIGHTS

Les ordinateurs de l'époque étaient aussi très lents, en particulier les lecteurs de disquettes (ou de cassettes !). Il fallait normalement attendre plusieurs minutes avant que le début du jeu soit chargé (bien plus qu'il n'en faut pour en télécharger l'intégralité avec un modem récent). Il existait pourtant des astuces logiciels pour accélérer les lecteurs. Il était également envisageable de compresser les données pour que moins d'accès au disque soient nécessaires. Les programmeurs de jeux se donnaient rarement la peine d'utiliser (ou même de comprendre :-) ces techniques, alors que les pirates se faisaient un point d'honneur de distribuer la version du jeux qui prendrait le moins de place possible et le moins de temps à se charger.

CHARGEMENT RAPIDE DE CHESSMASTER 2000

Il arrivait même parfois que des adaptations soient si mauvaises ou que les jeux soient si bâclés, que les pirates devaient y corriger certains bugs pour qu'ils soient vraiment jouables.

UNE COPIE BIEN FADE

Vous vous souvenez peut-être qu'Opération Flashpoint avait beaucoup fait parler de lui au moment de sa sortie, à cause de sa protection spéciale nommée "Fade". Au lieu d'afficher un message d'erreur lorsque le jeu se rend compte qu'il s'agit d'une copie pirate, il se dégrade progressivement (armes qui ne tirent plus droit, personnages qui se mettent à voler, etc.). Il devient ainsi en théorie beaucoup plus difficile d'obtenir un crack fonctionnel, et cela encourage également les possesseurs d'une copie pirate à aller acheter l'original lorsque le jeu devient injouable. En pratique, cela n'a pas empêché Opération Flashpoint d'être piraté sur le net, mais son développeur, CodeMasters, y croit toujours et annonce un prochain jeu de snooker où la gravité sera perturbée si le jeu se trouve copié. Mieux encore, on annonce des DVD équipés de la même technologie: le film s'arrêtera de jouer à un passage clé si ce n'est pas l'original! Y a pas à dire, les éditeurs ont de l'imagination, dommage que les pirates en aient toujours plus pour cracker leurs protections.

DEVENEZ CHASSEUR DE PRIMES

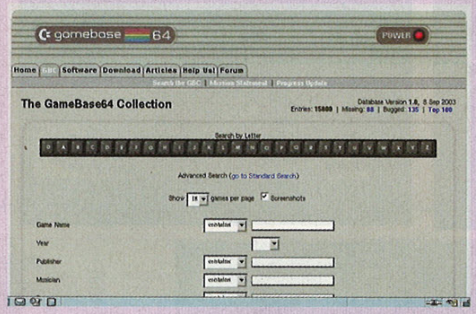
Et au lieu de traquer de dangereux criminels armés, ce sont les créateurs de virus qui seront votre cible. Microsoft aurait en effet promis pas moins de 250000$ à toute personne permettant de démasquer les auteurs des virus MSBlast et SoBig. Soi-disant que ces vers auraient causé du tort à Billou. Alors qu'il faut se rendre à l'évidence, c'est tout le contraire qui s'est passé: MSBlast a quand même forcé des milliers d'utilisateurs à corriger une faille de sécurité critique, ce que Microsoft n'aurait jamais réussi à faire sans son aide.

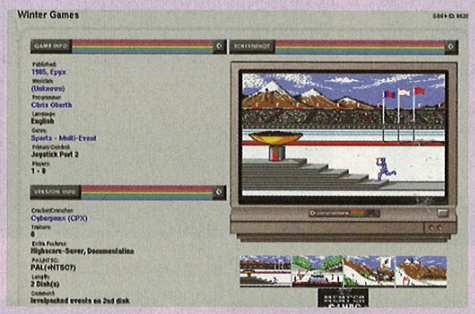
LES ÉMULATEURS C64
Si vous voulez voir à quoi ça ressemblait...

Vous ne pouvez pas tous ressortir le C64 qui traîne encore dans le grenier. Mais il est possible de faire tourner la plupart des jeux et des démos de cette époque sur son PC, avec un émulateur. Les meilleurs émulateurs du moment sont VICE (http://viceteam.bei.t-online.de/), CCS64 (http://www.ccs64.com/) et Frodo (http://www.uni-mainz.de/~bauec002/FRMain.html).

Pour une liste plus complète :
http://www.emu-france.com/?page=fichiers&idMachine=81
http://directory.google.com/Top/Computers/Emulators/Commodore/Commodore_64/

Vous trouverez aussi sur le Net la presque totalité des programmes qui ont été conçus pour cette machine. La meilleure adresse est sans doute la Gamebase64 (www.gb64.com) qui comprend plus de 15000 titres.





LA TRES COMPLÈTE BASE DE DONNÉES DE GB64.COM

Les jeux sont fournis sous la forme d'images de disquettes, des fichiers .D64, que vous n'avez plus qu'à charger dans votre émulateur. Ces titres font pour la plupart encore l'objet d'un copyright. Toutefois, les éditeurs n'ont plus beaucoup d'espoirs commerciaux à leur sujet et voient plutôt d'un bon oeil que des gens s'intéressent encore à leur travail. Il s'agit d'abandonware. Mais attention, même si vous ne risquez pas d'être inquiétés avec le C64, ce n'est pas le cas avec des jeux encore récemment commercialisés (surtout avec les consoles de jeux).
Il est aussi intéressant de noter que certains inconditionnels sortent toujours des jeux et des programmes pour cette machine. Regardez sur gamebase64.

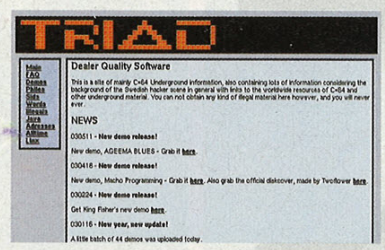
logiciels, un fournisseur d'originaux de choix pour eux, dont le chiffre d'affaire a commencé à couler dangereusement. N'ayant pas de moyen légaux pour se défendre, la société a émis des pressions sur divers membres du groupe. Finalement, Ixion, le leader, a décidé de ne plus rien distribuer en Suède, pour se concentrer sur la scène internationale et notamment les États-Unis.

LES 15 MINUTES DE GLOIRE

Actuellement, les pirates sont assez médiatisés. Mais à l'époque, le milieu était peu connu du grand public et on parlait peu de leurs exploits. En 1996, un groupe de hackers suédois avait piraté le serveur web de la CIA, pour soutenir un autre groupe suédois qui faisait l'objet d'une condamnation aux States. Les hackers avaient modifié la page d'accueil de la CIA (devenue Central Stupidity Agency) pour faire passer leur message et mentionnaient plusieurs liens vers la homepage de TRIAD. Plusieurs membres ont alors été suspectés et interrogés, mais c'était surtout la première fois qu'un groupe de C64 faisait un tel battage médiatique.

La plupart des photos d'écran qui illustrent ce dossier sont tirés d'oeuvres de TRIAD. Il était temps que Pirat'z rende hommage à ces pionniers. Et si l'on parle encore d'eux aujourd'hui, c'est moins pour les centaines de jeux qu'ils ont mis à disposition que pour leur créativité et leurs talents de programmeurs. Pensez-y.

TRIAD Homepage :



http://www.df.lth.se/~triad/triad/

HILARY CLINTON PIRATÉE EN CHINE

On sait que le marché du logiciel pirate va bon train en Chine. Et bien le livre y a droit aussi. Un peu partout, des marchands vendent sous le manteau, ou sur de petits étals, des éditions pirates des best-sellers, bien sûr, mais aussi des livres que la censure interdit dans le pays. Les amendes très sévères que les pirates risquent ne semblent pas beaucoup les troubler. Le livre de Hilary Clinton, Mon histoire, par exemple, se trouve déjà en une demi-douzaine de versions pirates en Chine. Les Etats-Unis vont-ils intervenir ?

LÀ, ILS PARTENT EN SCOUILLES

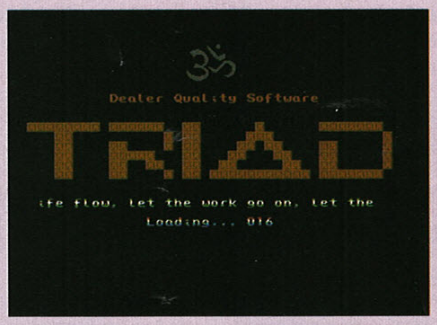
On vous parlait dans le précédent numéro de la société SCO, qui a décidé que Linux est illégal (il y aurait eu "emprunt non autorisé" de code source dans le kernel), et qu'IBM en particulier est le principal fautif. Après une nuit sans doute difficile, Monsieur SCO s'est levé en étant persuadé que la licence GPL violait la constitution américaine en allant à l'encontre du droit d'auteur. Il faut dire que Monsieur SCO a des problèmes de mémoire, et ne se souvient plus d'avoir distribué de nombreux produits sous licence GPL.

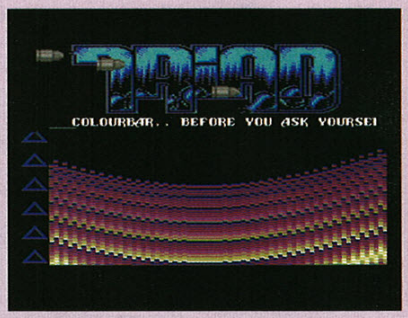
LE RETOUR DE LA REVANCHE DE NAPSTER

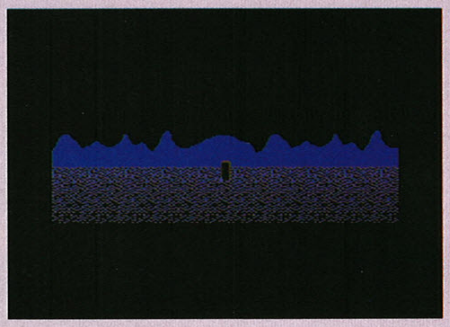
Au début octobre Napster a repris du service, mais il n'est accessible qu'aux utilisateurs payant un forfait mensuel ou à ceux qui désirent payer une à une les chansons téléchargées. Il y aura une version Premium de Napster qui offrira évidemment plus de services comme le téléchargement illimité et l'accès aux stations de radio. Cette base de données, qui aura pour concurrent l'iTune d'Apple (qui sera sur PC avant 2004), contiendra environ 500 000 chansons. Mais les gens veulent-ils vraiment débourser pour ce genre de service?

DÉMOS ET INTROS

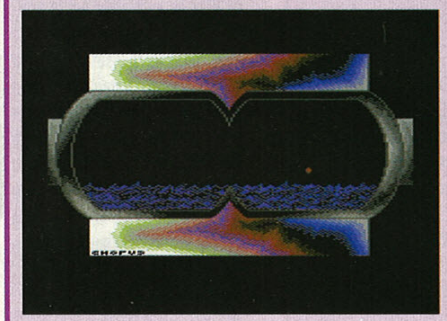
Tous les jeux étaient accompagnés de la signature des personnes qui l'avaient cracké, ça s'appelait une intro. On pouvait y lire des instructions pour le jeu, comment il avait été cracké et les états d'âme des pirates. La forme la plus simple d'intro consistait en un logo avec un texte défilant (scroll text) quelque part à l'écran. On appuyait alors sur une touche et le jeu se chargeait.
Comme c'était une sorte de carte de visite, les pirates tâchaient de soigner ces intros un maximum et vous en mettaient généralement plein la vue : des modes graphiques insoupçonnés, des animations dans tous les sens et des effets sonores impressionnants. Quand on regarde les copies d'écran de ces prouesses d'antan, on ne voit pas forcément ce qu'il y a d'extraordinaire. Pourtant les ordinateurs de l'époque étaient mille fois moins puissants que les PC récents. Sur C64, par exemple, il n'était en principe pas possible d'afficher plus de 2 ou 4 couleurs différentes (sur une palette de 16 !) dans une même zone de pixels, ou de dépasser la résolution de 320x200. Pourtant certains coders étaient capables d'afficher 128 couleurs en haute résolution avec des techniques d'entrelacement.
Lorsqu'ils avaient du temps, ils composaient aussi des oeuvres indépendantes plus longues : les démos. Organisées en plusieurs parties, elles faisaient se succéder différents effets programmés par les membres, comme s'ils se passaient la main.

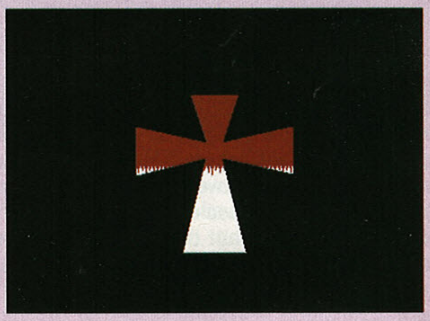






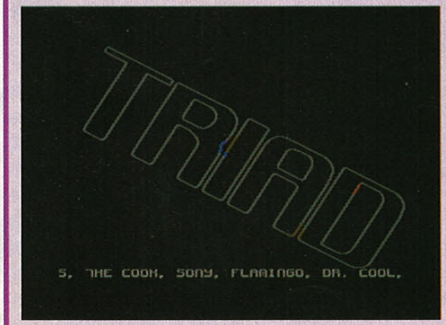
QUELQUES PARTIES DE LA DEMO UTOPIA





RED STORM

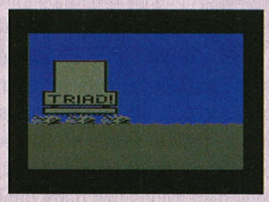
Les pirates étaient toujours très bavards. Les interminables scroll texts racontaient tout et n'importe quoi. Ils parlaient beaucoup de la scène, naturellement. Il n'y avait d'ailleurs pas une démo sans leurs fameuses salutations (greetings) à d'autres membres de groupes amis. Il arrivaient aussi qu'ils expriment leurs convictions politiques (le plus souvent anarchistes) ou philosophiques, ou toutes les sortes de sottises qu'ils trouvaient amusantes.

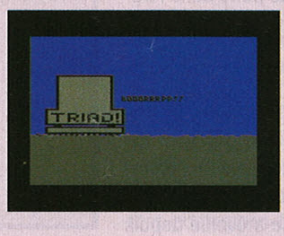


DÉMOS ET INTROS (suite)

Avec un extrait des scroll texts de Metalpart :

Certaines démos étaient aussi écrites pour exprimer la haine ou le mépris que l'on nourissaient envers un autre groupe. On voit ici combien TRIAD en veut à SCC.





FAUSSES NEWS ?

Vous avez sans doute été surpris par certaines anomalies dans les news de ce numéro. Il s'agit de news d'époque, traduites et compilés à partir de différents numéros du magazine électronique underground *Illegal* (http://fairlight.org/fanzines/). Ne vous y trompez pas : elles sont marquées du logo bleu de Commodore.

LES COPY-PARTY

Parmi les activités préférées des pirates des années 80, à part cracker des jeux ou programmer des démos, il y a les fêtes. Pas n'importe quelles fêtes : des rencontres de passionnés d'informatiques et de jeux vidéos. Organisées le plus souvent par des groupes importants, ces copy parties se déroulaient dans les lieux convenus à l'avance (hôtels, auberges de jeunesse, entrepôts et salles en tout genre) et pouvaient durer plusieurs jours.

On y échangeait des jeux, beaucoup. C'était l'occasion pour les groupes de distribuer leurs derniers cracks. Les gens apportaient aussi leurs ordinateurs et les meilleurs échangeaient aussi des idées et des techniques de programmation. En une ou deux nuits blanches, les pirates programmaient des démos, des animations et des effets spéciaux qu'ils laissent ensuite à la communauté comme un cadeau souvenir.

Les invitations se faisaient par les mêmes voies que celles par lesquelles les jeux piratés étaient distribués, c'est-à-dire entre gens de confiance (il était d'ailleurs de bon goût de coder des invitations animées au chargement des jeux). Il était assez rare que la police vienne pointer son nez à ces parties. Quand cela arrivait, des dizaines d'ordinateurs et des milliers de disquettes étaient saisis.

Il existe encore des copy parties aujourd'hui, mais leur intérêt est réduit à cause d'Internet qui facilite tellement les échanges. Par contre, les demo parties ou coding parties sont d'actualité. Les groupes y présentent, un peu comme à un festival, leur dernières créations sur écran géant. Les groupes d'utilisateurs de Linux font aussi ce qu'ils appellent des install parties, où ils aident les participants à installer ce système sur leurs ordinateurs.

CHARTS - AVRIL 1989

C64 GAMES

1 MICROPROSE SOCCER
2 PROJECT FIRESTART
3 F 16 TOMCAT
4 RUN THE GAUNTLET
5 TARGET RENEGADE III
6 NAVY MOVES
7 KATAKIS
8 FISH
9 CRAZY COMBAT
10 FIST

C64 CRACKERS

1 IKARI
2 FAIRLIGHT
3 X RAY
4 ELITE
5 711
6 DOUGHNUT CRACKING SERVICE
7 HOTLINE
8 A TOUCH OF CLASS
9 COSMOS
10 NATO

IZ

AMIGO AMIGA

JUST ICE, de IKARI, légende vivante, a déclaré dans leur dernière party qu'ils allaient pratiquement lâcher le C64. Et pourquoi ? Pour se concentrer sur l'Amiga, pardi. Mais quelle perte !

WEETBIX, le fameux cracker de SCG, est de retour. Mais devine : sur Amiga, pour en foutre plein la vue à ORACLE ! Mmmh, au moins la scène Amiga en Angleterre devient plus interessante...

LES ANGLAIS ENCORE DEVANT LES FRANÇAIS

Non, il ne s'agit pas de la coupe du monde de rugby, dont le résultat n'est pas connu au moment d'écrire cette news, mais de l'application de l'EUCD à la législation anglaise. L'EUCD, ou European Union Copyright Directive, dont on vous parle régulièrement dans le mag', est bien sûr le frère jumeau du DMCA américain, et était censé entrer en fonction dans tous les pays de l'Union Européenne avant le 22 décembre 2002. Donc oui, vous pouvez rire, les Anglais sont sacrément en retard. Mais moins que les Français, puisqu'on attend toujours cette loi chez nous. Remarquez, on n'est pas pressé: c'est le genre de loi qui risque de brider sévèrement la liberté d'expression, et de mener à de nombreux abus (le DMCA l'a bien montré aux USA). En tout cas, la loi est particulièrement sévère en Grande-Bretagne, où il n'y a même pas d'exception prévue pour la copie de sauvegarde: faire une copie personnelle d'un CD acheté devient du vol! Heureusement, j'ai confiance dans le gouvernement français pour faire traîner les choses, disons, encore un an s'il-vous-plaît?

BITTORRENT : LE NOUV

'Z

NOUVELLES DU FRONT

L'un des meilleur groupe d'Angleterre revient sur la scène et nous montre son talent avec plusieurs nouveaux cracks très cools. Je parle bien-sûr de SCOUSE CRACKING GROUP, avec WEETBIX, CHUNK, DR.J et MOG. Les Anglais retrouvent ici de puissants rivaux. FIRKIN, SMASH et GENE lachent ACTUAL CRACKING ENTERTAINMENT (contrairement à THE SILENTS, qui a rejoint ACE, l'a lâché, l'a rejoint et l'a finalement lâché pour de bon). Il fondent leur nouveau group : STARS.
IKARI a un nouveau membre : TRIDOS (viré de FUSION pour recracking) les rejoint..

EARTHSTATION5 REDESCEND SUR TERRE

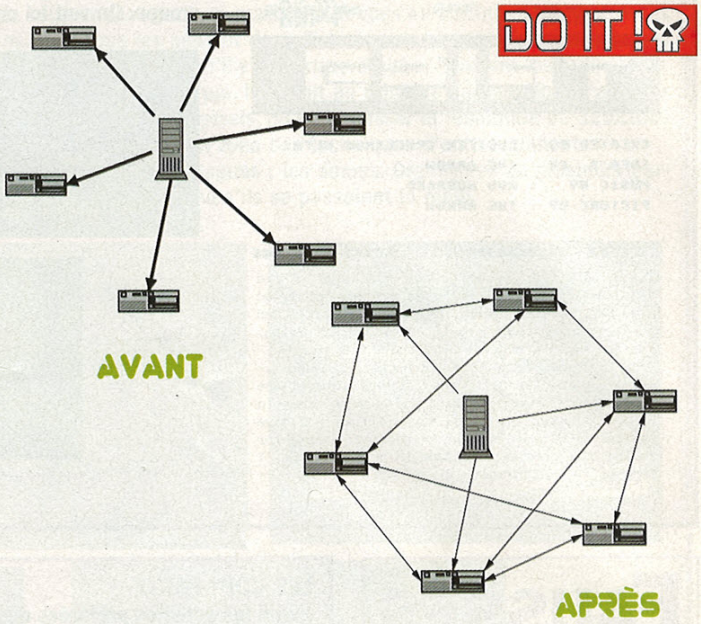
EarthStation5 (www.earthstation5.com) est sans doute le logiciel de P2P le plus laid de la planète. Et ce n'est pas son moindre défaut. Il a été en effet révélé sur la liste de sécurité Full Disclosure que le logiciel contenait du code permettant d'effacer n'importe quel fichier sur un ordinateur faisant tourner ES5, en envoyant une certaine commande à distance. Les détails sont sur :
http://lists.netsys.com/pipermail/full-disclosure/2003-October/011339.html, mais l'important est qu'il ne s'agit pas d'une simple vulnérabilité. C'est une fonctionnalité de ES5 qui a été implémentée volontairement par ses auteurs. Autant dire qu'ils n'ont pas eu l'air très malins après cette découverte, eux qui se prétendent des experts en sécurité. Evidemment, ils ont rapidement modifié le programme pour éliminer cette fonction suspecte, et ont ensuite fait de leur mieux pour trouver une excuse. Selon eux, ce mécanisme était utilisé dans la mise à jour automatique du programme. Peut-être pour "mettre à jour" automatiquement les logiciels concurrents au passage?

On pensait avoir à peu près tout vu dans le domaine du Peer-to-Peer (P2P), et pourtant il est un logiciel qui parvient enfin à renouveler le genre et prendre des parts de marché sur Kazaa et eDonkey. Ce logiciel, c'est BitTorrent, et puisque nous n'en avions pas parlé dans Pirat'z jusqu'à présent, il est temps de lui rendre justice.

Au commencement était Napster. Mais il a été crucifié, et même s'il a miraculeusement ressuscité récemment, tout le monde s'en fout (ce qui montre que l'homme a évolué depuis 2000 ans). Aujourd'hui, ce qui nous intéresse, ce sont ses concurrents. Les Américains, toujours aussi bouchés, n'ont d'yeux que pour Kazaa, tandis que les Européens ont compris qu'eDonkey et son eMule étaient quand même au-dessus. Autour de ces ténors gravitent les logiciels un peu plus exotiques, comme DirectConnect (www.neo-modus.com) et ses hubs spécialisés, FreeNet (freenetproject.org) et son anonymat, EarthStation5 (www.earthstation5.com) et ses backdoors... et BitTorrent (http://bitconjurer.org/BitTorrent), qui est celui qui nous intéresse ici comme j'espère que vous l'avez compris.

Qu'a donc BitTorrent de si particulier ? On pourrait le résumer par : "il n'y a pas de fonction de recherche". Attendez, ne fuyez pas, ça ne veut pas dire qu'on ne peut pas trouver ce que l'on cherche... Mais chaque chose en son temps, commençons par le début, c'est-à-dire l'idée de base derrière BitTorrent. En fait, l'auteur du logiciel a cherché à répondre au problème suivant : comment quelqu'un peut-il distribuer un fichier au monde entier sans faire exploser sa bande passante ? Le mettre en téléchargement sur son site web pose en effet le problème du coût de la bande passante, qui peut faire très mal si trop de gens téléchargent le fichier (il y a beaucoup d'exemples de pauvres gars qui ont été victimes du succès d'un gros fichier sur leur site et se sont retrouvés avec une facture plutôt salée de la part de l'hébergeur). La solution imaginée par BitTorrent consiste à mettre à contribution ceux qui téléchargent le fichier, pour leur faire uploader ce fichier en même temps aux autres personnes qui le téléchargent.

DO IT !

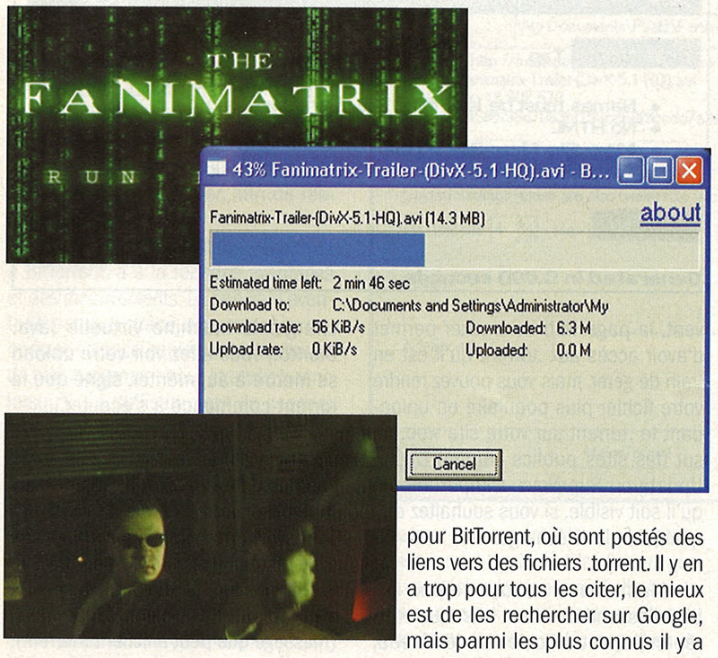


Concrètement, le système fonctionne de la manière suivante. Imaginons que la personne J veuille partager le fichier XXX. J crée un fichier portant l'extension .torrent (par exemple XXX.torrent), et le met à la disposition de tout le monde (sur son site web disons). Vu que c'est un petit fichier - entre 1 et 50 ko - ça ne posera pas de problème de bande passante. Si la personne R veut télécharger XXX, il n'a qu'à cliquer sur XXX.torrent sur le site web. BitTorrent lit alors XXX.torrent, dans lequel il trouve des informations sur le fichier à télécharger (taille, checksum, etc.) et surtout l'adresse d'un "tracker". Le tracker est un serveur qui stocke les informations sur qui est en train de télécharger XXX, où chacun en est de son téléchargement, ... BitTorrent se connecte donc au tracker et lui demande chez qui il peut télécharger XXX, et à partir de là le téléchargement commence.

BitTorrent insiste sur l'équité entre les utilisateurs du réseau : on partage forcément les fichiers que l'on est en train de télécharger, et on télécharge (à peu près) à la même vitesse que l'on uploade. C'est là-dessus que se base le protocole de BitTorrent pour garantir une efficacité maximale dans la distribution des fichiers.

Tenez, nous allons illustrer cette utilisation de BitTorrent en téléchargeant la bande annonce d'un film amateur, "The Fanimatrix: Run Program", une suite au premier volet de la trilogie "The Matrix". Commencez par télécharger BitTorrent sur http://bitconjurer.org/BitTorrent/download.html et installez-le. Ne vous inquiétez pas si vous ne trouvez pas de lien sur le bureau ni dans le menu démarrer : BitTorrent se lance tout seul lorsque l'on clique sur un fichier .torrent dans le navigateur (il est également possible de télécharger les fichiers .torrent et de double-cliquer dessus dans l'explorateur). Bien, maintenant rendez-vous sur http://fanimatrix.net, cliquez sur "Enter" puis "Download" et "Run Program Trailer". Tout en bas, dans "Filesharing links", cliquez sur le lien BitTorrent correspondant au fichier que vous voulez (MPEG ou DivX). Blam, une boîte de dialogue s'ouvre pour savoir où télécharger le fichier, et le téléchargement commence. 2 minutes plus tard, vous voilà avec une chouette bande annonce, et je vous laisse deviner comment télécharger le film entier ;-)Vous remarquerez la particularité des fenêtres de téléchargement de BitTorrent : il y a non seulement une vitesse de download, mais aussi une vitesse d'upload, car c'est pendant que vous téléchargez le fichier que vous êtes susceptible de l'uploader ailleurs. Dès que vous fermez la fenêtre, vous ne partagez plus le fichier ! Evidemment, il est de bon ton de ne pas fermer sa fenêtre dès son téléchargement terminé, mais d'attendre un peu, afin de laisser d'autres personnes télécharger chez vous. Petite astuce pour ceux qui souhaiteraient partager un fichier de nouveau après avoir fermé la fenêtre : il suffit de le re-télécharger au même endroit, BitTorrent se rend compte qu'il est déjà fini donc ne télécharge rien, mais la fenêtre réapparaît.

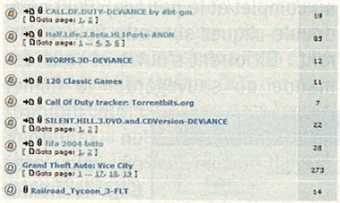
EAU COURANT PIRATE ?



AU TORRENT GOÛTANT

Bon, c'est bien beau tout ça, mais vous n'avez quand même pas lu tout ça juste pour télécharger Fanimatrix ! Non ? Et bien si, car le reste vous risquez fort de ne pas pouvoir le télécharger ! En effet, comme on pouvait s'y attendre sur un réseau pensé pour faciliter le transfert de gros fichiers, la majorité du trafic sur BitTorrent est généré par l'échange de fichiers piratés. Jeux, utilitaires, films, séries télé, MP3, tout y passe... si vous avez lu l'article sur le piratage de la GameCube et que vous vous demandez où les gens téléchargent leurs ISO, la réponse n'est plus très loin. Mais évidemment, hors de question pour nous de télécharger quoi que ce soit d'illégal. Nous allons juste nous contenter d'observer comment font tous ces internautes pour s'échanger des tonnes de matériel piraté au nez et à la barbe de la RIAA, de la MPAA et du Père Noël, qui du coup n'a plus rien à offrir le moment venu.

Ceux qui ont la conscience tranquille vont généralement utiliser BitTorrent comme il a été prévu de le faire, en mettant le fichier .torrent sur leur site, et c'est là que vous le trouverez. Les autres (c'est-à-dire pas mal de monde en fait, bande de pirates !) mettent leurs liens à la disposition de tous sur des sites dédiés. Vous connaissez ShareReactor (www.sharereactor.com) pour eDonkey ? C'est un site où on peut trouver des liens eDonkey vers tout plein de fichiers. Il existe le même genre de sites pour BitTorrent, où sont postés des liens vers des fichiers .torrent. Il y en a trop pour tous les citer, le mieux est de les rechercher sur Google, mais parmi les plus connus il y a notamment SuprNova : (www.suprnova.org) et Digital Update (www.digital-update.com).



Comme vous pouvez le voir, il y a de l'activité ! Evidemment, ce ne sont pas les seules sources de fichiers .torrent. Groupes Yahoo, canaux IRC, sites web plus privés... voilà autant d'endroits où s'échangent les précieux liens. Mais généralement, plus c'est underground, moins c'est légal, donc si vous décidez d'y fourrer le nez, c'est à vos risques et périls !

UN TORRENT VAUT MIEUX QUE DEUX TU L'AURAS

Vous êtes maintenant capable de télécharger à volonté, mais comment faire si vous souhaitez partager avec le monde entier votre dernière création artistique, ou votre dernier jeu cracké (jeu que vous avez écrit vous-même bien sûr). Malheureusement, la procédure est un peu plus compliquée que pour eDonkey et Cie.

La première étape est de trouver un tracker, ou d'en créer un. Pour ce qui est de la création, ce n'est pas ce qu'il y a de plus facile, donc pour l'instant, contentons-nous de chercher un tracker disponible. Les sites comme SuprNova ou Digital Update cités plus haut ont souvent leurs propres trackers qui sont mis à la disposition des internautes pour distribuer leurs fichiers. Vous pourrez trouver d'autres trackers en cherchant sur le net, en lisant régulièrement le groupe Yahoo "torrent-talk", ou sur des pages web recensant les trackers, comme celle de Filesoup : http://www.filesoup.com/trackerlist.html. Car, comme vous le remarquerez, les trackers les plus publics (comme ceux de SuprNova) affichent souvent complet ! Dans notre exemple, nous allons utiliser le tracker disponible sur http://pred2003.no-ip.org:6969, qui accepte tout type de fichiers (pensez à bien lire les règles d'utilisation d'un tracker avant de faire votre choix, et s'il n'y a pas marqué que toute personne est la bienvenue, il vous faut demander d'abord la permission au propriétaire du tracker). Dans notre cas, l'adresse du tracker est plus précisément http://pred2003.no-ip.org:6969/announce :

ET L'ANONYMAT DANS TOUT ÇA ?

On le sait depuis que le dernier numéro de Pirat'z s'est vendu à 3 millions d'exemplaires, l'anonymat est au coeur des préoccupations des internautes. Ceux-ci souhaitent en effet protéger leur vie privée, ainsi que leurs activités illicites, mais ça c'est secondaire, on est bien d'accord. Alors, si vous aussi ça vous chagrine, je ne saurais que trop ne pas vous conseiller BitTorrent, car il va vous être difficile d'être anonyme dessus. Vous pourriez essayer d'utiliser un proxy, mais ce n'est pas vraiment encore prévu, et vous allez avoir du mal à le configurer, sans parler de la perte de performances. Comme en plus des clients comme Azureus permettent de visualiser les adresses IP de toutes les personnes en train de télécharger un fichier, vous n'êtes pas vraiment invisible... Alors, imaginez qu'en plus, il suffirait que le FBI lance son propre tracker public pour récupérer les IP de milliers d'internautes et espionner leurs activités... Haha, j'en vois qui se précipitent sur leur micro pour fermer leurs transferts, tout en pestant contre ce p*** de Pirat'z qui aurait pu le dire avant ! Trop tard, j'ai votre adresse, gnark gnark gnark...**

'Z BRÈVES

C'est le pognon qui gouverne ! GOLLUM et THE SARTGE (ex-FAIRLIGHT) on présenté leur nouveau jeux RUBICON. Il sont toujours à la recherche d'un éditeur, mais on peut déjà se demander qui va cracker ce jeux !?
Des nouveaux sur la scène Amiga : BLACK MONKS. Il nous donne une belle série de cracks avec R-Type et The Kristal.
MIRCALE (No. 1 au Danemark, il parait) nous montre ce qu'un bon cracker peut faire : The Deep, et en une partie ! On dirait que MIRACLE est le nouveau STEVE de ZENITH.
Une release plus décevante en provenance du Danemark : un groupe nommé KEFRENS, avec Lords of the Rising Sun. Vous aurez sans doute remarqué qu'il ne s'agit que d'un preview... Ça n'aurait pas posé de problème s'ils l'avaient mentionné dans l'intro, mais ils ne l'ont pas fait.

DOCUMENTS AUTO DESTRUCTIBLES

Parmi les nouvelles fonctionalités de Office 2003, on nous annonce un nouveau système de protection des documents (centralisé vers les serveurs de Microsoft !). On peut choisir, par exemple, quels destinataires ont le droit de lire un message, et meme faire en sorte qu'un document s'auto-détriuse au bout d'un certain temps !
Mais ceux d'entre vous qui utilisent régulièrement les produits de M$ savent que, justement, les documents qui disparaissent, ce n'est pas une nouveauté.

DO IT !

AOL COMBAT LE SPAM... A SA MANIÈRE

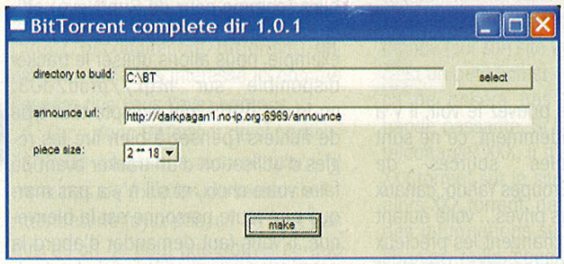
Vous avez certainement connu ces publicités s'affichant non pas dans une fenêtre de l'explorateur, mais par le service de messages de Windows. On vous a expliqué précédemment comment les éviter (si vous l'avez raté, la solution la plus simple est de désactiver le service d'affichage de messages). Mais tous les utilisateurs d'AOL ne nous lisent pas, et ils ont continué de se plaindre auprès de leur fournisseur... lequel a décidé de faire tout simplement la manip' à leur place! En effet, AOL a d'abord créé un petit programme que ses abonnés pouvaient utiliser pour stopper les pubs, mais presque personne ne l'utilisait. Finalement, ils ont donc installé une mise à jour de leur logiciel qui va directement modifier la configuration de Windows pour stopper le service incriminé. Et ceci sans même en avertir l'utilisateur! AOL se défend en disant que personne ne s'est plaint, mais la méthode laisse quand même à désirer. 15 millions d'abonnés ont déjà été "désactivés" à leur insu. Bientôt, AOL va discrètement remplacer IE par Netscape, et personne ne s'en rendra compte...

TÉLÉCHARGEZ HIDDEN & DANGEROUS

L'idée de fournir gratuitement au téléchargement de vieux jeux commence à faire son chemin. Cette fois-ci, c'est rien de moins que le superbe Hidden & Dangerous que vous pouvez télécharger en toute légalité. Les développeurs ont en effet estimé que cela permettrait de promouvoir Hidden & Dangerous 2, que vous pouvez également télécharger sur le net, mais moins légalement. Quoi qu'il en soit, si vous aimez les jeux d'action - stratégie, foncez sur http://www.file-mirrors.com/search.src?file=hddeluxe.exe pour trouver où télécharger ce classique.

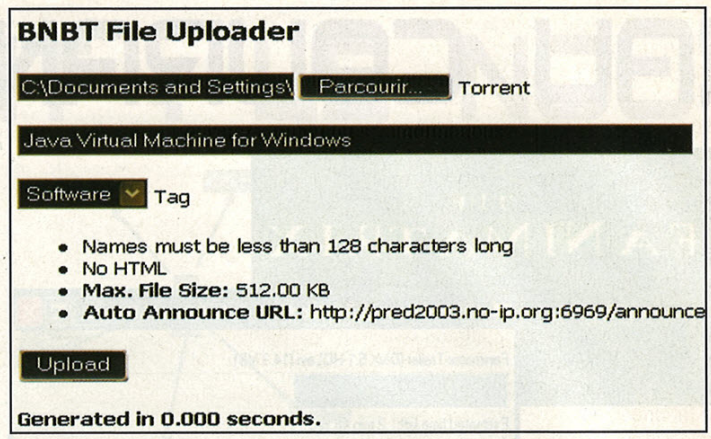
c'est l'adresse qu'il faudra indiquer dans le fichier .torrent, mais l'adresse sans le "/announce" correspond au site web du tracker, sur lequel vous trouverez différentes informations comme les règles, les fichiers actuellement partagés, les statistiques, etc.

Maintenant, sur la page web de BitTorrent, téléchargez le programme "CompleteDir", qui va nous servir à créer le fichier .torrent, et installez-le. Il est sensé placer un raccourci dans le menu Démarrer, mais si comme moi vous ne le trouvez pas, allez le dénicher dans C:\Program Files. Créez un répertoire (par exemple C:\BT) sur votre disque dur, dans lequel vous mettrez le ou les fichier(s) que vous souhaitez partager (si vous voulez partager un répertoire, mettez ce répertoire dans C:\BT). Lancez ensuite CompleteDir, et remplissez les champs : "directory to build" = C:\BT, "announce url" = http://pred2003.no-ip.org:6969/announce. Pour "piece size", vous pouvez laisser la valeur par défaut. Si ça vous intéresse, ça représente la taille des morceaux découpant le fichier : comme eDonkey, BitTorrent découpe chaque fichier en petits morceaux afin d'optimiser la coopération entre les utilisateurs. Plus les morceaux sont petits, plus le transfert sera optimisé, mais aussi plus votre fichier .torrent sera gros (ce qui, bien sûr, n'a pas grande importance). Cliquez sur "make", et voilà, un fichier .torrent apparaît dans C:\BT !



Ce fichier, vous allez devoir le rendre disponible sur le net. Le plus important est de le faire d'abord accepter par le tracker. Rendez-vous sur la page du tracker, et cherchez le bouton "Upload". Généralement, il vous faudra d'abord vous enregistrer (bouton "Signup"), car le tracker n'acceptera que des fichiers d'utilisateurs reconnus. Sélectionnez le fichier .torrent à uploader (et pas le gros fichier que vous souhaitez partager, attention !), indiquez ce que c'est, et voilà, c'est presque fini :]

Comme pouvez le remarquer sur la capture d'écran, j'ai décidé de partager la machine virtuelle Java pour Windows, que Microsoft ne distribue plus parce qu'ils sont en colère contre Sun et veulent couler Java et le remplacer par .NET, ces salauds. Mais bon, vous vous en foutez, donc continuons. Car il faut bien que quelqu'un vienne télécharger votre fichier .torrent pour que tout ça serve à quelque chose. Souvent, la page web du tracker permet d'avoir accès aux .torrent qu'il est en train de gérer, mais vous pouvez rendre votre fichier plus populaire en uploadant le .torrent sur votre site web, ou sur des sites publics comme Digital Update ou SuprNova. L'important est qu'il soit visible, si vous souhaitez que quelqu'un le télécharge.

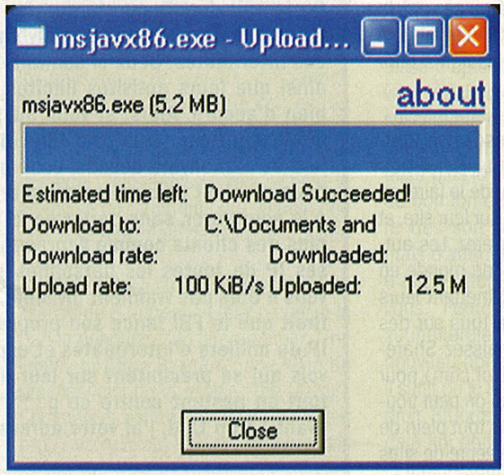


Maintenant, surtout ne pas oublier l'essentiel : il faut bien que vous répandiez votre fichier sur le réseau, donc que vous le partagiez. Vous allez être le premier "seeder" (un seeder est quelqu'un qui a le fichier au complet et le partage). Pour cela, double-cliquez sur votre fichier .torrent : BitTorrent s'ouvre et vous demande où sauvegarder le fichier cible. Indiquez un répertoire où vous avez déjà le fichier au complet (C:\BT dans notre cas). BitTorrent scanne alors le fichier, se rend compte qu'il est déjà là, et affiche "Download Succeeded". Surtout, NE FERMEZ PAS LA FENETRE ! Vous êtes maintenant prêt à uploader le fichier aux milliers d'internautes avides de télécharger la machine virtuelle Java. Bientôt, vous allez voir votre upload se mettre à augmenter, signe que le torrent commence à s'écouler...

Vous pouvez rencontrer quelques petits soucis au cours de ces manipulations. En particulier, les trackers publics sont souvent surchargés : soit ils ne vous laisseront pas uploader de fichier car ils ont atteint leur limite, soit ils renverront parfois un "Connection Refused" (message que peut afficher BitTorrent), ou encore auront des problèmes à afficher leurs pages web. Dans ces deux derniers cas, insistez jusqu'à ce que ça fonctionne, ce n'est qu'une question de patience.

TORRENT EN PLAN

Mais, vous demandez-vous, que se passe-t-il si vous décidez malgré tout de fermer cette fenêtre BitTorrent qui encombre votre espace ? Si votre fichier a été suffisamment populaire, à ce moment plusieurs personnes ont eu le temps de le télécharger entièrement, et ils deviennent les nouveaux seeders. D'ailleurs, la règle dans la communauté BitTorrent est de ne pas fermer la fenêtre avant d'avoir uploadé un minimum (au moins la quantité téléchargée). Cette règle assure que le fichier se propage bien et que le torrent ne se dessèche pas... ce finit par arriver lorsqu'il n'y a plus aucun seeder.



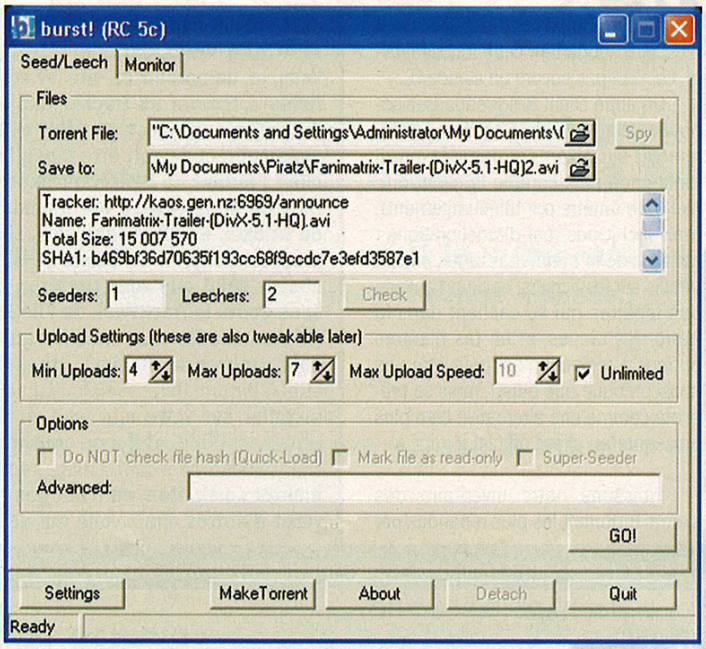
Pour comprendre ce phénomène, il faut examiner l'évolution d'un torrent. Au début, il n'y a typiquement qu'une seule personne qui a le fichier au complet. Ceux qui le téléchargent n'ont donc pas une bonne vitesse de téléchargement. Mais une fois que plusieurs personnes ont fini de le récupérer, et qu'il y a donc plus de seeders, le fichier peut être téléchargé très rapi-

dement. Il y a donc de plus en plus de seeders... jusqu'à ce que les gens en aient marre et ferment leur fenêtre BitTorrent. Lorsque (presque) plus personne ne télécharge le fichier, le nombre de seeders diminue, et au bout d'un moment le torrent est déclaré "mort" lorsque le dernier seeder disparaît. C'est à ce moment que l'on peut voir sur les forums des gens réclamer un "reseed", c'est-à-dire que quelqu'un avec le fichier au complet se remette à le partager, afin de ressusciter le torrent.

Ce principe d'évolution, particulier à BitTorrent, a à la fois des avantages et des inconvénients. Le principal avantage est que grâce au protocole coopératif efficace implémenté, la vitesse de téléchargement peut être très bonne lorsqu'il y a suffisamment de seeders et de personne en train de le télécharger simultanément. Comme de plus il n'est pas très pratique de partager des fichiers (il faut laisser une fenêtre ouverte par fichier), les gens ne partagent que peu de fichiers. Cela évite les files d'attente interminables que l'on trouve sur eDonkey, où on se fait de toute manière toujours systématiquement déconnecter quand on arrive enfin en première place ;) L'esprit de la communauté BitTorrent est également (pour l'instant) plus orienté partage que sur eDonkey, où nombreux sont ceux qui arrêtent de partager un fichier dès qu'ils en ont fini le téléchargement, ou même utilisent des clients hackés qui leur évitent d'avoir à uploader. Et le résultat est là : on télécharge généralement bien plus vite que sur eDonkey. Evidemment, il y a un revers à la médaille, tout n'est pas rose comme le saumon dans le torrent. Le partage de fichier étant assez malaisé, les gens partagent beaucoup moins de fichiers que sur eDonkey. Le contenu n'y est donc pas aussi varié, et ce sont essentiellement les dernières nouveautés qui sont disponibles. Les fichiers plus vieux, eux, disparaissent avec le torrent qui les a générés. Autre inconvénient de taille : l'absence de fonction de recherche. Il faut visiter les sites soi-même, ou utiliser Google et avoir de la chance, afin de trouver ce que l'on cherche. C'est sûr que c'est un peu moins pratique que de taper un texte dans une fenêtre de recherche universelle...

TORRENT ALTERNATIF

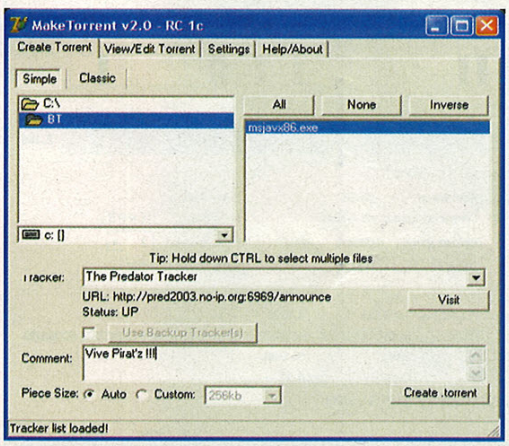
Pour remédier aux défauts du client BitTorrent officiel, qui est quand même assez minimal côté interface graphique, un certain nombre d'autres clients ont été développés. Comme il y en a un bon paquet, je ne vais vous parler que des plus populaires. Commençons par burst!, disponible sur : http://krypt.dyndns.org:81/torrent/.



Il permet notamment de voir à partir du fichier .torrent quels sont les fichiers que l'on va télécharger, quelle est l'adresse du tracker, de savoir combien de seeders et de leechers (ceux qui téléchargent en ce moment) il y a. On peut aussi limiter sa bande passante utilisée (attention, plus l'upload est bas, plus le download sera lent, comme sur eDonkey). L'avantage principal étant peut-être de pouvoir regrouper tous ses transferts au sein d'une seule fenêtre (les fenêtres DOS qui s'ouvrent peuvent être cachées dans l'onglet "Monitor", ou automatiquement en cochant "Start Transferts Hidden" dans le menu "Settings").

Le petit ami de burst! est MakeTorrent, du même auteur, qui se télécharge au même endroit (je vous laisse trouver le lien sur la page, vous y arriverez, hein ?). C'est un programme, qui, comme son nom l'indique, sert à créer des fichiers .torrent, comme CompleteDir donc. Mais il est bien plus complet que CompleteDir : il tient à jour une liste automatique de trackers publics, à laquelle on peut rajouter ses propres trackers privés. Il permet également d'éditer les fichiers .torrent (pour changer le tracker par exemple), et supporte même une fonctionnalité que le client officiel n'avait pas prévue : les "backup trackers", c'est-à-dire la possibilité d'utiliser plus d'un tracker, au cas où le premier choix aurait des problèmes. C'est cool, mais vu que pour l'instant seuls deux clients non officiels (burst!

UN TORRENT, ÇA TRAVERSE UN PARE-FEU ?
Mais oui, évidemment, c'est de l'eau après tout... BitTorrent a essentiellement besoin des ports 6881 à 6889, qu'il utilise pour ses transferts. Si vous êtes derrière un firewall, il vous faudra donc lui permettre d'utiliser ces ports, ou au moins l'un d'eux (mais plus il y en a d'ouverts, plus vous pouvez télécharger de fichiers simultanément). Si vous accédez à internet par un réseau local, il vous faudra rediriger ces ports sur la machine servant de passerelle vers votre ordinateur. Sous Windows avec le partage de connexion internet, vous trouverez ça dans l'onglet "Avancé", bouton "Paramètres" de la connexion. Si vous n'y arrivez pas, écrivez-nous, on fera un hors-série spécial sur le sujet.



MS iTUNES (1)

À la sortie d'iTunes pour Windows (qui donne donc accès au magazin de musique online de Apple), Microsoft ne rate pas l'occasion de prêcher pour sa paroisse." Les utilisateurs de iTunes sont limités à la musique provenant de Apple's Music Store," regrette David Fester de MS. iTune n'étant compatible qu'avec l'Ipod, il argue que les utilisateurs de Windows sont habitués aux choix, celui des services et des périphériques qu'ils utilisent. Et au choix du traitement de texte, du navigateur, et du système d'exploitation ?

ARTISTES MAUDITS

Après la première vague d'internautes visés par la RIAA pour le partage illégal de musique, le site Slyck dédié au P2P (www.slyck.com) a mené une petite étude, et s'est rendu compte que la RIAA n'avait pas frappé au hasard. En effet, certaines chansons revenaient plus souvent sur les disques durs des personnes accusées. La chanson de Busta Rhymes, "Pass the Courvoisier", était par exemple la plus représentée. Si j'étais vous, je me spécialiserais tout de suite dans les chansons folkloriques roumaines, c'est moins risqué.

LE VIRUS WANADOO

Il ne s'agit pas d'une publicité de l'opérateur, mais d'un virus qui se ballade sur le réseau eMule. Il mesure 435k, est écrit en delphi et se cache sous des noms comme AOL Hacker 2004, Hotmail Hacker 2004, Portable Orange (FT) Keygen, WinZip All Version Keygen, Sexy ScreenSaver 2004, Alcohol 120% 1.4.8.1009 CORE Keygen ou Wanadoo Hacking Tool 2004 (d'où le nom !).
Le plus amusant, c'est qu'il affiche un message qui dit que le fichier est corrompu et qu'il faut se procurer une nouvelle version du programme.

DO IT !

ON SE DÉFEND COMME ON PEUT

Après l'échec du fournisseur d'accès américain Verizon qui a dû finalement dévoiler l'identité de ses internautes coupables d'avoir partagé quelques MP3 de trop, ce sont des universités du Massachusetts qui ont été sommées de vendre leurs étudiants. Finalement, elles n'auront pas à le faire, ce qui a réjoui de nombreux opposants de la RIAA, mais la raison est quand même assez limite: les demandes venaient de l'état de Washington, et ne pouvaient donc pas s'appliquer au Massachusetts. Une victoire aux points d'une certaine manière.

COUPABLE D'AVOIR UNE TOUCHE ?

L'universitaire J.A.Halderman a rédigé une étude sur un système de protection qui vient de sortir, MediaMax CD3. Ce système consiste en un driver qui s'installe lors de la première lecture (avec un autorun). Ce driver, entre autre, empêche la copie du disque. Cependant, il suffit de maintenir la touche SHIFT enfoncée lors que l'on insère le disque pour que ce driver ne soit pas chargé, et donc faire sauter la protection.

Ce n'est pas la seule faiblesse révélée dans l'étude. Pour une version 3, c'est pas brillant. Mais que voulez-vous, la protection CD, du moment que l'on peut écouter les morceaux (donc les enregistrer), est vouée à l'echec par nature.

Le plus étonnant dans cette histoire, c'est que certaines lois qui restreignent le droit de copie, notamment aux Etats-Unis, interdisent la détention de tout dispositif électronique ou logiciel qui permettrait de passer un système de protection. Pour être logique, il faudrait retirer tous les claviers du marché... Encore une preuve de l'absurde et de l'inefficacité de la plupart des mesures prises contre le piratage.

et ShadOw's Experimental que l'on verra plus loin) supportent cette fonctionnalité, ce n'est pas encore un standard.

Un autre client BitTorrent assez populaire est celui de ShadOw, à télécharger sur http://bt.degreez.net. Il fonctionne plus comme le client officiel (une fenêtre par téléchargement), mais inclut pas mal d'améliorations : contrôle de la bande passante, pause, détails sur les fichiers, backup trackers, des fenêtres qui se cachent dans la barre des tâches, et un tas d'autres options à régler. Il n'est peut-être pas aussi pratique que burst!, mais se présente comme une alternative bien plus puissante au client officiel.

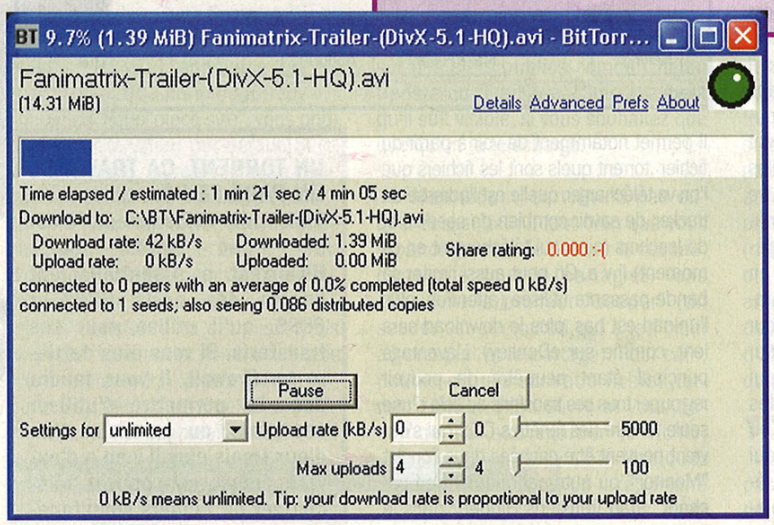
Finissons notre inventaire des clients BitTorrent les plus répandus par Azureus, disponible sur : http://azureus.sourceforge.net.

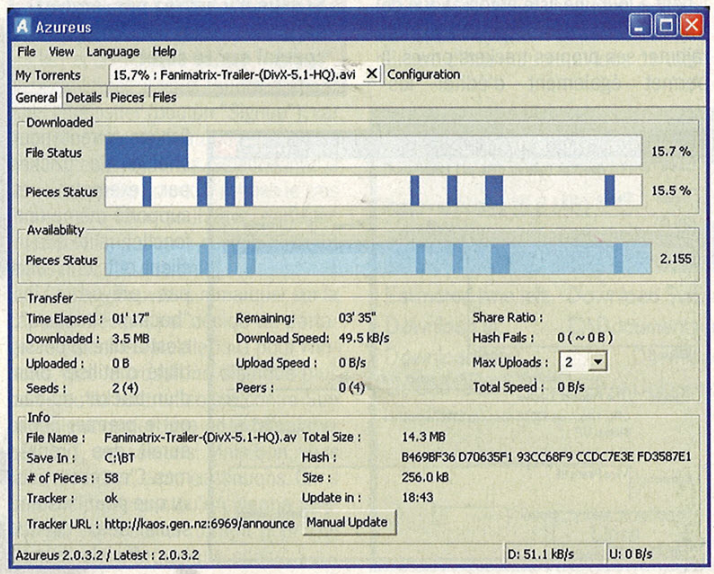
Sa particularité est d'être en Java, donc pensez à télécharger Java si vous ne l'avez pas déjà installé sur votre machine (le lien est sur la page d'Azureus). Sinon, Azureus ne se lancera pas et n'affichera pas de message d'erreur, ce qui n'est jamais très rassurant. Mais croyez-moi, ça vaut la peine de faire un petit effort pour essayer Azureus, car c'est sans doute le client le plus impressionnant. Vous y trouverez toutes les options disponibles ailleurs, avec en plus notamment : choix de la langue (français compris), client IRC intégré, interface de téléchargement similaire à un Kazaa ou eDonkey (avec affichage de la disponibilité des différents morceaux du fichier), la possibilité de choisir quels fichiers télécharger lorsqu'il y en a plusieurs pour un seul .torrent (on peut ainsi récupérer des fichiers à partir d'un download incomplet), et surtout, le redémarrage automatique des transferts et partages en cours afin de ne plus avoir à s'en occuper manuellement... Voilà certainement le client BitTorrent le plus complet à ce jour !

Enfin, il existe d'autres outils plus ou moins utiles, que vous trouverez si vous vous intéressez de plus près à BitTorrent. Citons des programmes de trackers (voir l'encadré à ce sujet), un programme permettant de créer un seed à sur un serveur web (WebSeed, sur http://bt.degreez.net), et un logiciel original proposant de créer des torrents sans trackers en s'appuyant sur les autres réseaux P2P (TorrentAid, www.torrentaid.com). Je vous laisse le soin de me tester tout ça ;-)

TRACKER VAILLANT...

Vous le comprendrez vite si vous souhaitez partager vos propres fichiers, trouver un tracker fiable est souvent l'étape la plus lourde du processus. C'est en effet la limitation principale de BitTorrent, mais celle-ci devrait être singulièrement diminué dans un futur proche : l'auteur de BitTorrent annonce en effet des modifications subtiles du code réseau qui diminueraient d'un facteur 100 la charge du tracker. En attendant, vous serez peut-être tenté d'installer votre propre tracker. Il en existe plusieurs, et je vous laisserai le soin de choisir celui que vous préférez. Un des plus simples à installer est sans doute le TrackPack de FileSoup : www.filesoup.com/trackpak.html (il vous faudra vous inscrire aux forums et fouiller un peu dedans pour trouver le fichier). Un autre kit tout en un se trouve sur http://bittorrentkit.sourceforge.net. PHPBTTracker est un tracker PHP à installer sur votre site web, et sa page officielle est http://dehacked.2y.net:6969, et il a un cousin qui fait la même chose, BitGrog, sur www.rumandwater.com/bitgrog, sans parler de phpTracker qui devrait bientôt sortir. Bon, ce n'est pas tout, cherchez bien et vous en trouverez d'autres, mais voilà qui devrait vous suffire pour commencer.





TORRENT CONTINU

À ce point, vous devez avoir compris que BitTorrent n'est pas un client à prendre à la légère, et que sa popularité n'est pas usurpée. Il a réglé un problème récurrent du P2P - comment avoir une fonction de recherche efficace - en l'éliminant purement et simplement, et en se concentrant sur la question "comment avoir un taux de transfert optimum et distribuer au mieux les fichiers". Résultat : une communauté plus soudée qu'autour des autres clients P2P, et un nouveau mode à part de distribution de fichiers. Nul doute que BitTorrent a un bel avenir devant lui, en tout cas, tant que la RIAA n'en aura pas entendu parler...

KHAN

GRAND CONCOURS PIRAT'Z
GAGNEZ UNE N-GAGE NOKIA

Pour participer au concours, c'est très simple, il vous suffit de trouver les réponses à ces trois questions :

Question 1 : Dans quel programme se trouvait la vulnérabilité qui a permis la prolifération récente du vers MSBlast ? (Entourez la bonne réponse.)

A- Les services RPC **B- Internet Explorer** **C- Solitaire**

Question 2 : Quel a été le premier groupe pirate à ajouter un menu " triche " aux jeux copiés ?

A- Microsoft **B- Triad** **C- Fairlight**

Question subsidiaire : combien de fois la lettre " Z " est-elle imprimée dans ce numéro de Pirat'z ?
Attention, tout compte (majuscule et minuscule, dans le texte, dans les illustrations...)

Le gagnant sera le premier, cachet de la poste faisant foi (date et heure) à nous avoir adressé sa réponse. En cas d'ex-æquo (bonne réponse postée le même jour à la même heure) le N Gage sera attribué au candidat le plus jeune.

Découpez soigneusement la page et renvoyez-la à : CONCOURS N_GAGE Publia, 2 bis rue Dupont de l'Eure 75020 Paris.
Nom : ..... Adresse : .....
..... Date de naissance : ..... Mail : .....

Indépendamment du concours, nous vous demandons de bien vouloir répondre à ces quatre questions, qui nous permettront d'améliorer le journal dans le sens de vos attentes :

- **Quels magazines de hack lisez-vous ? Donnez-leur une note sur 10.**

Pirat'z : ... /10
.... /10
.... /10

- **Dans Pirat'z , souhaitez-vous (entourez vos choix) :**

- plus de News / moins de News
- plus de Gamez / moins de Gamez
- plus de Hack / moins de Hack
- ne changez rien

- **Souhaitez-vous que les articles de Pirat'z deviennent :**

- plus simples
- plus techniques
- ne changent pas de niveau

- **Enfin, pourquoi lisez-vous Pirat'z ?**

.....
.....
.....

GAME CUBE : LES JEU

Le piratage sur GameCube, voilà quelque chose que Nintendo ne tenait pas à voir de sitôt, et qui tardait d'ailleurs à pointer le bout de son nez. Mais ça y est, le nez est sorti cet automne, et il est fort probable que le reste suive bientôt, à moins que Mario n'impose un hiver trop rigoureux. Car le petit plombier, c'est bien connu, n'apprécie guère les pirates !

LECHATKITU

GAMECUBE EMULATOR

Des émulateurs de GameCube, vous en trouverez plein sur le net, si vous prenez la peine de chercher "gamecube emulator" sur Google. Vous pourrez notamment mettre la main sur DolWin, mais vous ne pourrez pas faire grand-chose avec. Vos espoirs reposeront donc plutôt sur Dolphin, un nouvel émulateur dont vous pourrez trouver des vidéos sur le net, censées prouver que Zelda et Mario commencent à tourner un peu. C'est bon signe, mais l'expérience nous rendant méfiant, nous attendrons une version plus avancée avant de crier victoire.

GAMECUBE LIVE

Côté jeu en ligne sur GameCube, c'est un peu limite, à part Phantasy Star Online il n'y a pas grand-chose à se mettre sous la dent. Ce qui limitait jusqu'à présent pas mal l'intérêt de l'adaptateur réseau haut débit. Plus maintenant, vous me direz, avec l'apparition des hacks pour jouer à des jeux copiés, mais vous avez un article sur le sujet, donc c'est d'autre chose que je vais vous parler ici. Si vous suivez la Xbox, vous connaissez sans doute le logiciel gratuit XBConnect (www.xbconnect.com), qui concurrence le Xbox Live de Microsoft en permettant de jouer en ligne aux jeux prévus pour le réseau local. Et bien, un clone vient d'apparaître sur GameCube. Nommé Warp Pipe (www.warp-pipe.com), il n'est pour l'instant qu'en version alpha loin d'être optimisée, mais prévoit de supporter Kirby Air Ride, Mario Kart: Double Dash et 1080°: Avalanche. Evidemment, il vous faudra un de ces jeux, l'adaptateur haut-débit, un PC pour faire tourner Warp Pipe, ainsi qu'un routeur, avant de pouvoir essayer ce logiciel. Il faut bien ça pour être à la pointe du progrès!

Avant de rentrer dans les détails, une petite mise au point. Malgré mes incessantes tentatives pour vous inciter à nous écrire de jolies lettres d'injures, j'ai été assez déçu sur ce point-là... à l'exception d'un inconditionnel de son Nintendo GameCube qui ne supportait pas d'entendre "la" GameCube. Si c'est aussi votre cas, bouchez-vous les oreilles, ou passez un logiciel d'OCR sur le scan du mag' puis faites un chercher / remplacer. Car je ne saurais être tenu responsable de vos toilettes bouchées si vous piquez une crise de rage contre notre cher magazine. Ceci étant dit...

GAMECUBE ET PIRATAGE : PASSÉ, PRÉSENT ET AVENIR

Depuis la sortie des trois consoles "nouvelle génération" (Xbox, PS2 et GameCube, par ordre d'analphabétisme), la grande question que tous les indécis se posent avant de faire leur choix a toujours été : "mais est-ce qu'on peut y mettre un modchip ?". Ce n'est pas forcément la bonne question, parfois il vaut mieux se demander s'il y a de vrais jeux dessus, mais bon, tant pis pour vous si vous avez acheté une Xbox. Au moins, vous avez Linux et le démineur... mais je m'égare, le fait est que la GameCube faisait bien pâle figure à côté des multiples solutions de piratage disponibles chez ses concurrentes. Il y a bien eu des annonces plus ou encore plus bidon, de personnes ayant réussi à jouer à un jeu copié, à créer un modchip sans soudures, ou encore à finir Men in Black 2 sans mourir d'ennui. Bref, rien de très crédible. En juin, les groupes pirates s'étaient amusés à sortir sur le net les images ISO (images de CD) des jeux GameCube, mais sans moyen d'y jouer, c'était à peu près aussi frustrant

X COPIES SONT LA !

qu'un film interdit aux lecteurs de Pirat'z sur Canal+ sans décodeur. Et même plus, l'imagination n'étant pas suffisante pour en jouir.

Et puis la solution est venue en deux temps. Tout d'abord, avec la sortie de PSUL cet été : cet utilitaire a été conçu pour permettre aux développeurs amateurs d'exécuter du code sur leur GameCube. La méthode se rapproche de ce qui a été fait sur Xbox, où on exploitait une faille dans la gestion des sauvegardes dans un jeu pour provoquer un buffer overflow. Cette fois-ci, c'est un peu plus compliqué, puisque la faille ne concerne pas les sauvegardes, mais le code réseau du jeu Phantasy Star Online. En faisant se connecter le jeu à notre PC au lieu du serveur de jeu, il est possible d'envoyer du code réseau mal formaté de manière à provoquer un buffer overflow et exécuter du code arbitraire sur la console. PSUL se télécharge un peu partout, par exemple sur www.gcdemos.com.

Un peu plus tard, cet automne, le feuilleton continuait avec un nouveau programme : ACL, pour "Animal Crossing Loader", créé par le groupe pirate Eurasia. Comme son nom l'indique, le but de ce programme était initialement de permettre de charger l'ISO du jeu "Animal Crossing" sur sa GameCube. Finalement, il a été modifié et amélioré afin de pouvoir charger d'autres jeux. Le processus, sur lequel nous reviendrons bientôt plus en détail, est le suivant : PSUL est utilisé pour exécuter le "loader" sur la GameCube, loader qui communique avec le serveur lancé sur le PC pour télécharger les données de l'image ISO vers la GameCube, et lancer le jeu.

Evidemment, il y a plusieurs inconvénients à cette méthode, qui font qu'elle ne se répandra sans doute pas comme technique de piratage de masse (ouf, dit ici Mr. Nintendo). Tout d'abord, il faut le jeu Phantasy Star Online et l'adaptateur modem haut débit. Il faut aussi un ordinateur qui devra être connecté à la console pendant qu'on joue. Plus embêtant encore, la vitesse de transfert des données de l'image ISO sur le disque de l'ordinateur vers la console n'est pas suffisante pour atteindre la vitesse normale de lecture d'un jeu GameCube. Par conséquent, certains jeux souffrent de problèmes dans les séquences cinématiques, les voix ou les musiques, où survient un hachage assez désagréable. La sauvegarde ne fonctionne pas non plus dans quelques jeux. D'autres ne tournent même pas du tout. Bref,

tout n'est pas rose, et pour plus de détails sur ce qui marche et sur ce qui ne marche pas, direction http://gc-compat.webhop.net.

Alors, que nous réserve le futur ? Pour le savoir, faites le 3617 PIRATZ, à seulement 0,15 euro la seconde. Nous proposons une vaste collection d'horoscopes, tirages de cartes, lectures individuelles de boules de cristal, etc. Pour le retour de l'être aimé, de la chance et de Pirates Mag' dans les kiosques, allez voir ailleurs. Non, ce qui nous intéresse ici, c'est l'avenir du piratage sur GameCube. Ne doutons pas que ce que nous voyons aujourd'hui n'est que le début. Si Phantasy Star Online a pu être exploité, peut-être d'autres jeux seront-ils aussi vulnérables. D'autre part, pour l'instant il n'existe aucun outil "grand public" pour créer ses propres images ISO, mais cela ne devrait plus tarder (il y en aura sans doute au moment où vous lisez cet article). En effet, s'il est possible d'exécuter du code sur la console, il est possible d'écrire un logiciel qui lise les données sur le disque GameCube, puis les envoie sur le PC pour créer une image. De tels logiciels sont déjà annoncés, attendons donc... Côté modchips, il y a aussi des annonces, mais comme rien n'a encore été confirmé, mieux vaut ne pas trop s'avancer. Mais qui sait, des avancées ont également été faites dans le domaine de l'étude du BIOS de la console, ce qui prépare le chemin aux futurs modchips... et aux futurs procès de Nintendo.

ISO MODE D'EMPLOI

Après ces considérations générales, voyons plus précisément comment faire pour jouer à un jeu GameCube dont on possède l'ISO. Evidemment, pour rester dans le légalement correct nous supposerons que vous avez obtenu cette image à partir de votre jeu original. Si ce n'est pas le cas, vous n'avez pas le droit de lire ce qui suit. Vous vous demandez pourquoi je perds mon temps à l'écrire dans ce cas? Moi aussi.

Quoi qu'il en soit, la première étape est de connecter correctement votre PC et votre console. Configurez la connexion réseau local de votre PC pour avoir l'adresse IP 192.168.1.100 avec comme masque de sous-réseau 255.255.255.0. C'est tout, pas besoin d'indiquer de DNS (branchez quand même le câble réseau croisé qui reliera l'adaptateur haut-débit à la carte réseau de votre PC, ça fonctionnera mieux).

Ensuite, il faut configurer Phantasy Star Online (PSO dans la suite) et sauvegarder ces options, afin de ne plus avoir à le refaire à chaque fois.

'Z

PAPA, JE PEUX UTILISER KAZAA ?

"C'est mon prof qui a dit que j'en avais besoin pour faire mes devoirs". Il faudra bientôt recourir à ce genre de ruse pour pouvoir utiliser les réseaux P2P aux Etats-Unis, en tout cas si une certaine proposition de loi passe au Congrès. Celle-ci veut imposer l'autorisation parentale pour les logiciels de P2P, afin de préserver nos chérubins de la pornographie qui y rôde. L'intention est louable, mais comment s'assurer que c'est bien un parent qui click sur "Yes"? On a déjà suffisamment de mal avec la signature du bulletin scolaire..

ALLEZ DIRECTEMENT EN PRISON...

Une petite news qui nous vient directement de chez Ratiatum (www.ratiatum.com). Une nouvelle directive européenne serait en préparation, qui accentuerait singulièrement les mesures prises à l'encontre des utilisateurs de P2P. Un mineur pourrait ainsi se retrouver en prison pour avoir téléchargé un MP3 sur le net. Ce qui dérange notamment, c'est que cette directive soit soutenue par la femme de Jean-René Fourtou (PDG de Vivendi Universal), qui est au parlement européen. Pas très rassurant, mais bon, le temps que ça arrive en France...

PREMIÈRE MONDIALE : DES PIRATES AU PÉNAL

Habituellement poursuivie en vertu code civil la piraterie passe désormais au pénal. Ainsi, pour la première fois au monde, trois hommes risquent des peines de prison en Australie pour avoir violé la législation sur les droits d'auteur. Ils avaient piraté de la musique en ligne.

IZ

COPIE RÉVOLUTIONNAIRE... OU RÉACTIONNAIRE?

La compagnie FarStone vient de mettre au point un logiciel "révolutionnaire" dédié à la copie de jeux. GameCopy est disponible pour la modique somme de 60$, et est sensé permettre de copier la quasi-totalité des titres du marché, même protégés par SafeDisc, SecuROM ou LaserLock. Tiens, ils ont oublié StarForce on dirait... Mais qu'importe, ce logiciel "unique" ne semble pas plus intéressant qu'un bon vieux CloneCD, BlindWrite et Cie, dont on peut télécharger des versions d'évaluation sur le net. FarStone, faut quitter l'âge de pierre!

MS ITUNES (2)

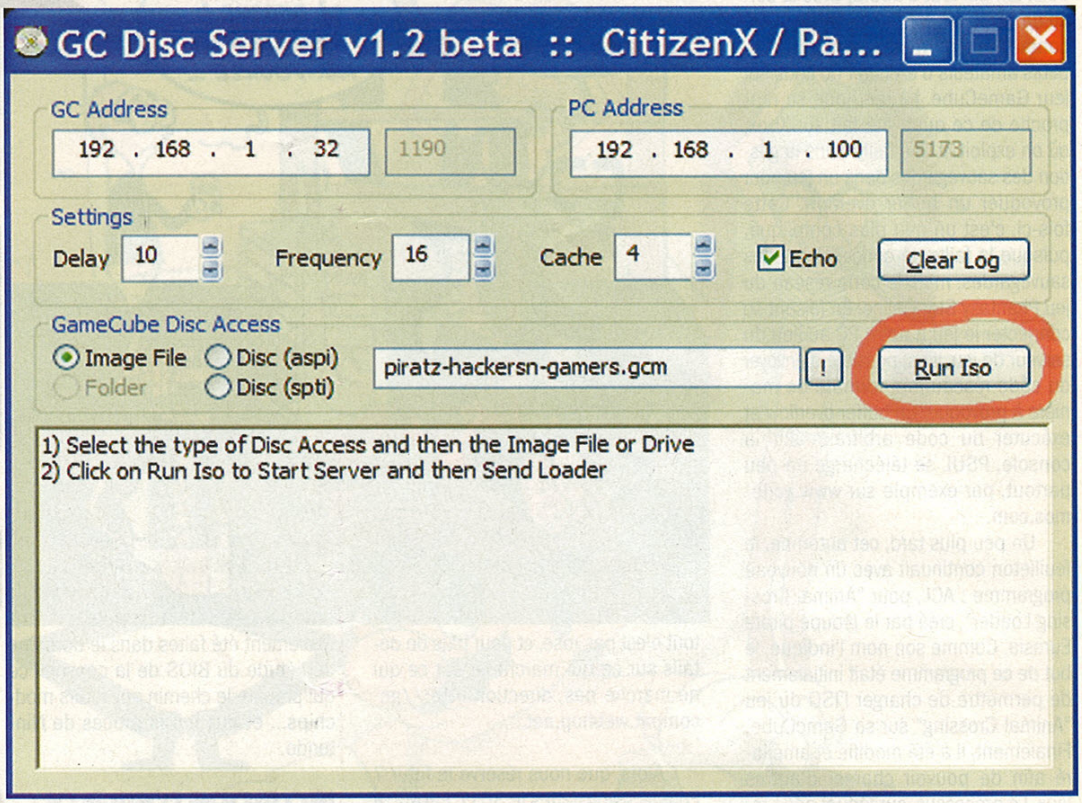
La vente de musique online par Apple a été le premier service payant à avoir réellement séduit les internautes et à les avoir fait décrocher du peer2peer. Mais maintenant que iTunes débarque sur les plates-formes Windows, les spécialistes (IDC) craignent que les pirates s'en mêlent sérieusement. D'abord, les mécanismes de protection de Apple sont volontairement légers pour faciliter l'utilisation. Mais surtout, les utilisateurs de Windows sont d'après eux plus bidouilleurs et moins scrupuleux que les adorateurs de la pomme...

WIRELESS : WPA ? BOF

Pas de miracle pour la nouvelle norme wireless WPA, sensée plus sécurisée que le WEP. Un expert aurait réussi à utiliser une méthode permettant de trouver la clé utilisée par le système PSK (Pre-Shared Keys) servant à l'authentification d'une session sur un réseau WPA. Cette méthode repose sur la capture de quatre paquets spécifiques seulement sur le réseau permettant de reconstituer la clé PSK. Or, il en fallait plusieurs milliers pour retrouver une clé WEP d'une taille de 64 bits ! Attention :cette faille ne fonctionne pas pour les architectures utilisant un serveur d'authentification indépendant.

Après avoir lancé PSO, allez dans les options réseau, rubrique "provider". Dans les options de configuration, choisissez de spécifier vous-mêmes l'adresse IP et de ne pas vous déconnecter automatiquement. Ensuite, entrez 192.168.1.32 comme adresse IP, 255.255.255.0 comme masque de sous-réseau, et 192.168.1.100 (l'adresse de votre PC donc) comme passerelle par défaut et DNS primaire. Ensuite, sauvegardez vos options sur la carte mémoire. L'étape suivante n'est nécessaire que si vous n'avez pas encore joué online à PSO. Vous allez avoir besoin de PSUL : ouvrez une fenêtre DOS sur votre PC (tapez cmd dans démarrer / exécuter), rendez-vous dans le répertoire de PSUL et tapez psul -s. Sur la GameCube, choisissez de faire une partie online et créez un nouveau personnage quelconque (inutile de se souvenir des mots de passe et compagnie). Sauvegardez votre perso sur la carte mémoire... le jeu démarre, et sur votre PC, PSUL devrait afficher "Saving user info on memory card... Done...".

Bien, le plus dur est fait, les étapes que nous venons de voir ne sont à faire qu'une fois, il ne reste plus qu'à jouer ! Téléchargez un loader sur internet (au moment où j'écris, il en existe



plusieurs, le dernier est le "PDX GameCube Disc Server 1.2 beta" du groupe ParadoX - vous pouvez aussi jeter un œil du côté de ce loader graphique : www.rypp.net). Là, il vous faudra regarder la doc pour voir comment ça fonctionne, mais ce que fait le loader, c'est d'une part uploader un petit loader (en extension .dol) sur la GameCube, d'autre part mettre en place un serveur sur le PC, auquel se connectera le loader GameCube pour télécharger l'image du jeu. Avec le premier loader du groupe Eurasia, il fallait faire tout ça à la main, ce qui était un peu lourd, mais le dernier loader de Paradox par exemple fait tout tout seul. On choisit l'image (qu'il est même maintenant possible de graver sur un CD ou un DVD pour économiser de la place sur le disque dur), un p'tit clic sur "Run Iso" et c'est parti !

Une fois que tout est prêt côté PC, ne reste plus qu'à lancer PSO sur sa console et démarrer une nouvelle partie online... lorsque le jeu va chercher à se connecter au PC, celui-ci va exploiter la faille dans le code réseau pour uploader le loader sur la console, et ainsi lancer l'ISO. Ne reste plus qu'à attendre, ce qui peut parfois être assez long (là, il faut jouer avec les options, et prendre son mal en patience).

MAIS QUE FAIT LA POLICE ?

Rien, pour changer. Par contre c'est Nintendo qui commence à paniquer un peu. Pour preuve des rumeurs assez contradictoires. D'un côté, il aurait été annoncé que l'adaptateur haut-débit pour la GameCube allait être abandonné, afin d'éviter d'autres détournements de son utilisation. Une nouvelle version de Phantasy Star Online serait aussi en préparation, qui corrigerait ce malheureux bug réseau (mouais, vu comme le jeu a dû se vendre depuis l'annonce de la faille, moi si j'étais développeur, je ferais exprès de laisser un tel "bug", qui serait malencontreusement découvert quelques mois plus tard...). Mais tout cela ne serait que rumeurs, une autre voix nintendesque annonçant qu'au contraire Nintendo allait supporter l'adaptateur haut-débit avec d'autres jeux... C'est donc un certain flou qui règne en ce moment, et nul doute que PSO et son adaptateur haut débit vont se retrouver sur bien des listes de Noël. D'ailleurs, c'est le moment de demander aussi un PC à ses parents, après tout, la console c'est bien, mais sur un PC, on peut aussi travailler, c'est bien connu ;-)

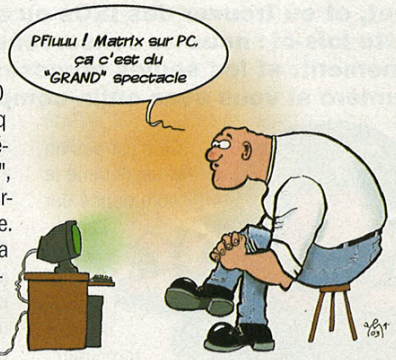
KHAN

ATTENTION !
C'est illégal de copier les images des CD, sous forme d'ISO ou autre, de jeux que vous ne possédez pas. Mais vous avez le droit de faire une copie de sauvegarde d'un jeu que vous avez acheté.

LA PROTECTION ANTI-PIRATE DE MATRIX REVOLUTIONS

Matrix 2 était trop bien classé au top des films... les plus piratés. La Warner semble avoir retenu la leçon et a finalement pris ses précautions pour le troisième et dernier volet. Des arrestations préventives en masse ? Des filtres spéciaux à la projection ? Non, c'est plus malin que ça, vous allez voir.

Matrix Revolutions a pulvérisé tous les records de lancement de l'histoire du cinéma en rapportant plus de 200 millions de dollars de recette en cinq jours. C'est bien sûr l'une des conséquences de l'opération " heure zéro ", qui consistait à faire sortir ce film partout dans le monde à la même heure. Mais une chose est sûr : la Warner n'a pas dépensé autant d'argent pour assurer cette synchronisation parfaite uniquement pour établir ce record (ni pour soulager la frustration des plus impatients, d'ailleurs). C'est une mesure contre le piratage.



Pourquoi les films sont-ils piratés ? Ce n'est pas vraiment une question d'argent. Les gens qui peuvent se payer un ordinateur et une connexion haut-débit ont, a priori, les moyens d'aller au cinéma de temps en temps. Ce n'est pas non plus une question de confort. A part pour les agoraphobes et les bricoleurs, un salon ne vaut jamais une salle de cinéma. On a plutôt recours au piratage, parce que ça permet de voir les films avant leur sortie en salle. On veut " tout, tout de suite ", mais on dirait que les marchands ne sont pas toujours à la hauteur du credo qu'ils essayent de faire avaler aux consommateurs.

En général, les films sortent plusieurs mois à l'avance aux États-Unis. C'est pourquoi les " screeners " (voir encadré) ont un tel succès en Europe, malgré leur piètre qualité. Pire, les fuites dans les maisons d'édition ou dans la presse font circuler dans le marché pirate des versions de qualité maximale. Or cela représente un manque à gagner important pour les éditeurs : si le film est mauvais ou s'il ne vaut pas la peine, les personnes qui en ont vu une version pirate ne vont pas payer pour le revoir en salle.

Pour Matrix Revolutions, la Warner a décidé de ne pas provoquer de délai intercontinental et donc de supprimer une des cause du piratage : l'effet avant-première. Non content de ça, les projections pour la presse ont été menées sous haute surveillance : contrôle sérieux des invitations, fouilles au corps, avertissements.

On a pourtant vu circuler, avant la sortie, des copies pirate de Matrix 3 sur les réseaux Peer2Peer. Seulement, à première vue, il ne s'agissait que de " fakes " (voir encadré). Par contre, nous avons voulu savoir combien de temps mettraient les français pour partager un screener du film. Nous avons ainsi placé un moniteur sur le site filedonkey.com. Et en effet, c'est seulement au bout de trois jours, le 8 novembre, un peu avant midi, qu'un screener en français est apparu lors de la recherche.

On dirait bien que la Warner a réussi son coup. Et pour une fois qu'un mesure anti-pirate ne nuit pas aux consommateurs normaux, il faut saluer le geste. Mais quand on voit sur le Net l'avis de beaucoup de fans déçus, on se demande si la Warner, consciente des faiblesses de son film, n'a pas voulu aussi prévenir les effets catastrophiques d'un bouche à oreille trop négatif.

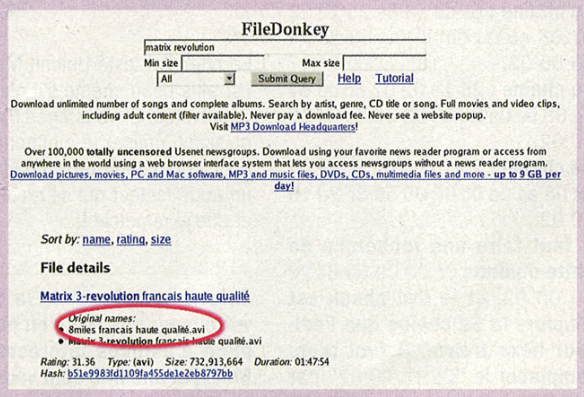
DE BAZANDE

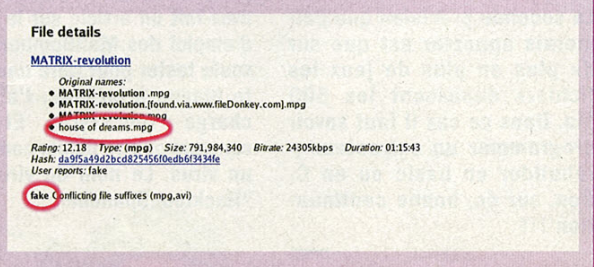
LES " SCREENERS "

Les screeners sont des films filmés : quelqu'un est allé au cinéma avec une caméra vidéo et a filmé l'écran pendant toute la scéance. La vidéo a ensuite été compressée et partagée sur le Net. La qualité de ces copies est, vous vous en doutez, assez médiocre – et je ne vous parle pas des gens qui passent devant la caméra... Mais certaines personnes sont si impatientes de voir un film qu'elles se contentent de ça.
Notez que parfois on utilise la bande son d'une version screener avec l'image tirée d'un DVD. On peut ainsi obtenir une version française d'un DVD américain, par exemple.

LES " FAKES "

Les réseaux de peer to peer sont pollués par des faux. On peut trouver un film porno sous le nom du dernier Disney, ou une version finlandaise à la place d'une version française. C'est assez ennuyeux pour les pirates, quand on sait que le téléchargement d'un film peut prendre plusieurs jours. Mais quand on y pense, ça arrange bien les éditeurs. On sait déjà que les majors de l'industrie du disque paye des gens pour distribuer des mp3 sans intérêt sous des noms plus séduisants, pour semer la confusion sur les réseaux de partage. Il est fort probable que les géants du film utilisent aussi de tels procédés. Mais il me semble plus raisonnable de penser, au contraire, que ces faux proviennent en majorité des utilisateurs.
Certains types de réseau P2P, notamment DirectConnect, demandent aux utilisateurs de partager un minimum de données pour pouvoir s'y connecter. Le minimum peut se fixer en terme de mégaoctets, ou en nombre de films de telle catégorie. Dans ces conditions, il peut être intéressant pour un utilisateur (de toute façon sans scrupule, puisqu'il pirate les films) de faire croire qu'il possède certains titres, alors qu'il s'agit d'autre chose. Certains sites pirate pensent aussi accroître leur popularité en distribuant de prétendues nouveautés.
On peut observer facilement ce phénomène sur filedonkey.com. Le réseau eDonkey, comme la plupart des systèmes de partage, utilise un hash pour identifier les fichiers. Ce hash est calculé en fonction du contenu du fichier, et ne dépend pas de son nom. Lorsque l'on fait une recherche, on peut avoir la liste de tous les noms de fichiers avec le même hash. C'est une manière efficace d'identifier un " fake ". Voyez vous-mêmes.





COURRIER DES LECTEURS

L'adresse n'a pas changé, c'est toujours sur piratgamez@yahoo.fr que vous pouvez nous contacter. Autre chose qui n'a pas changé, malgré ma tentative du dernier numéro, c'est le nombre de mails concernant les anciens numéros, l'abonnement, notre site internet, et où trouver des ISOs ou autres... Bref, si le message n'était pas clair, j'espère qu'il le sera plus cette fois-ci : nous ne conservons pas les anciens numéros, il n'y a pour l'instant ni site internet ni abonnement, et les seules adresses que nous fournissons sont celles du mag'. On verra dans le prochain numéro si vous avez enfin compris ;-)

Tout d'abord salut à toi !! Ensuite ton journal est super, continue comme ça, il déchire. Bon je t'écris parce que tes infos sur le rip des jeux ps2 sont totalement dépassées, notamment en ce qui concerne les dvd checks. Il y a pour les jeux actuels 2 dvd checks dans chaque exécutable. Le premier n'apparaît qu'une fois dans l'exécutable. La chaîne à chercher avec l'éditeur hexa est celle-ci: 00 11 3c 30 00 b2 ff 2d 80 80 00. Il faut la changer en : 00 11 3c 30 00 b2 ff 01 00 10 24.

La seconde chaîne à chercher est un peu différente mais reste très simple à trouver. La forme de celle-ci peut changer mais la plupart du temps elle ressemble à ça (ici pour Toca Race Driver) : 1re chaîne trouvée pour 0c 00 00 50 8c 2d 10 00 02 25 10 43 00 68 dd c4 8e 08 ee 0d 0c 00 00 50 8c 2d 10 00 02.
2e chaîne : 25 10 02 02 68 dd 64 8c 08 ee 0d 0c 00 00 50 8c 2d 10 00 02.
3e chaîne : 6c dd 64 8e 25 10 22 02 08 ee 0d 0c 00 00 50 8c 2d 10 00 02.
4e chaîne : 25 10 02 02 6c dd 64 8c 08 ee 0d 0c 00 00 50 8c 2d 10 00 02.
5e chaîne : 25 10 02 02 6c dd 64 8c 08 ee 0d 0c 00 00 50 8c 2d 10 00 02.
Il faut faire une recherche de cette chaîne : 0c 00 00 50 8c 2d 10 00 02, et le dvd check est toujours la 5e chaîne que l'éditeur hexa trouve. Il faut alors remplacer le "2d 10 00 02" par "14 00 02 24".
La seconde précision que j'aimerais apporter est que sur de plus en plus de jeux les fichiers dépassent les 500 Mo. Dans ce cas il faut savoir programmer un extracteur / rebuilder en basic ou en C. Bon, sur ce, bonne continuation !!!

DRCD

Bon ben merci, il n'y a pas grand-chose à rajouter, sinon que cette remarque judicieuse concernait l'article paru dans le numéro 3 sur le rip de jeux PS2.

Hi you ! Je viens de découvrir votre mag et il est vraiment bien, comparé à d'autres (vous êtes pas cher et assez complet). Voilà voilà, c'est au sujet des Mailbombers, bah c'est juste une p'tite remarque, vous en avez pas trouvé de plus moche ? Bon d'accord c'est fait juste pour envoyer des mails mais coté design... je vous conseille Unlimit Mail, il est très joli, et puis il est en français.

OPHÉLIE

En effet, j'ai testé Unlimit Mail et il est plus beau, même s'il n'est pas très évolué. Si vous cherchez plus puissant, utilisez le mailbomber X-Mas, qui m'a été recommandé par un autre lecteur qui se reconnaîtra et que je remercie !

Salut à vous tous !!! Je trouve votre magazine riche en news et plein d'astuces intéressantes. Mais j'ai une info dont vous faire part. Dans votre numéro 4, vous avez fait un article sur le mode d'emploi des MailBombers. J'ai voulu tester pour faire une petite blague à un pote. J'ai téléchargé QuickFyre. Et j'ai constaté que ce fichier contenait un virus. Le nom du virus est "Hacktool.Spammer".

SNIPER

Ce n'est pas un virus, comme le nom donné par l'antivirus l'indique : "Hacktool.Spammer" signifie qu'il s'agit d'un outil de spam. L'antivirus le détecte car un individu mal intentionné pourrait l'installer sur ton ordinateur pour pouvoir spammer à partir de ta machine. Mais si c'est toi qui l'as installé, pas de risques...

Bonjour, j'ai lu votre article affirmant qu'on peut trouver l'adresse IP d'un PC distant à partir du numéro de téléphone (ou de l'adresse email). J'aimerais bien qu'on m'explique en détail comment on fait SVP. Autre problème que je rencontre : j'ai beau chercher un site où on peut surfer anonymement, je n'y arrive pas. En effet, sur ces sites, il y a toujours des surprises, soit on ne peut pas accéder à sa messagerie ou sur les pages sécurisées https ou encore il faut payer quelque chose pour aller où on veut ! Je cherche un moyen (pas 36 mais un seul !) pour surfer anonymement partout sur internet et gratuitement, c'est tout ! Quel est-il SVP ? Merci pour votre coup de main.

ODICE3000

Je ne sais pas trop où tu as trouvé un article disant qu'on pouvait retrouver l'IP à partir du téléphone, mais si on a bien écrit ça, j'aimerais savoir où ! À partir du mail, ça se fait en examinant les en-têtes du mail afin de trouver l'IP de la personne qui l'a envoyé. En effet le serveur de mail la dévoile le plus souvent (pas toujours, ce n'est par exemple pas le cas pour Hotmail). Par exemple, dans les en-têtes de ton email, il y a :
Received: from [80.15.xx.yy]
by web20506.mail.yahoo.com
via HTTP; Mon, 25 Aug 2003
07:35:06 PDT
On peut en déduire que ton IP est sans doute 80.15.xx.yy. Adresse que je peux taper sur http://visualroute.visualware.co.uk pour voir que tu es sans doute un abonné de Wanadoo dans la région parisienne.
Quant à trouver un site pour surfer gratuitement partout sur internet sans soucis : ça n'existe pas à ma connaissance, sinon il aurait été cité dans notre article anonymat. Si vous en connaissez un, faites-nous signe !

Bonjour, j'ai lu dans votre mag 4 le dossier sur l'anonymat, très intéressant. J'ai voulu essayer de passer par un proxy. Cela n'a pas fonctionné. Je possède une connexion illimitée chez AOL et un modem 56Kb sous Win98.

FGFGF

Le fin mot de l'histoire, qui pourra intéresser d'autres lecteurs : AOL ne supporte pas l'utilisation de proxies, il vous faudra installer un autre navigateur (comme Netscape) si vous souhaitez être invisible sur le net.

Comment passe-t-on dans le courrier des lecteurs ?

BOB

En posant des questions intéressantes. Ou très bêtes. Je te laisse deviner à quelle catégorie la tienne appartient.

KHAN

Le Best-of du net Pirati'z

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

HACKING et SECURITÉ INFORMATIQUE

iSecureLabs. Actualité en français sur le hacking et la sécurité : www.isecurelabs.com
Packetstorm. Tous les exploits, outils, failles... en anglais : packetstormsecurity.nl
K-Otik. Toutes les vulnérabilités, en français : www.k-otik.com
Input Output Corporation. Une team qu'on l'aime bien : www.ioc.fr.st
Anonymat. Se cacher sur le net : www.anonymat.org
Stay Invisible. Si vous cherchez un proxy : www.stayinvisible.com
Ouah. Docs "spécialisées dans l'intrusion réseaux UNIX". Très technique : www.ouah.org
Securis. Libertés, freewares pour vous protéger: securis.info
Phrack. L'e-zine de référence des hackers, en anglais : www.phrack.org
Zone-H. Actualité des activités pirates : zone-h.org
SecuriteInfo. Le nom est explicite : www.securiteinfo.com
Crayon. Là aussi, le nom... ;) www.crayon.fr.fm
Madchat. Vision d'underground : www.madchat.org
Tenka.fr.st. Un site en français autour du hacking : www.tenka.fr.st
CyberArmy. Hacking, anonymat, libertés. En anglais : www.cyberarmy.com
NSA. Les espions américains qui nous surveillent : www.nsa.gov
DGSE. Les français qui surveillent les ricains : www.dgse.org
Dicofr.com. Un dictionnaire des termes techniques en informatique : www.dicofr.com

SAUVEGARDE et DEVELOPPEMENT

-Génériques

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

-Copie (gravure, modchips, ...)

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

-Spécifiques à certaines machines

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

TELECHARGEMENT et ACTU PIRATE

-Web

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

-Peer-to-Peer

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

-FTP, News et IRC

SmartFTP. Un client FTP gratuit : www.smartftp.com
newzBin. Traque pour vous les binaries postées sur les News : www.newzbin.com
mIRC. Le client IRC le plus répandu : www.mirc.com
Invision. Un mIRC bourré aux vitamines : invision.lebyte.com

ABANDONWARE et EMULATION

-Abandonware

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

-Emulation

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

JEU ONLINE

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

CHEATS

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

HORS-SÉRIE N°3 SPÉCIAL DON'T DO IT

PIRAT'Z

HACKERS & GAMERS

Hors-série Tout gratuit

2€

Tout Gratuit

Les nouvelles méthodes des pirates pour ne pas payer

Les chaines payantes
les jeux vidéos, les DVD
internet, la musik
LE CINÉMA, les logiciels

DEJA EN KIOSQUE

L 19302 - 11 - F: 1,50 € - RD

DOM 1,80 € - BEL 1,90 € - CH 4,50 FS - CAN 2,95 $ can - MAR 25 dh