

HACKER news Magazine

SKYPE



Le TELEPHONE GRATUIT

LE MAGAZINE 100% SECURITE



Cartes de CREDIT
ATTENTION DANGER!



Emmanuel Goldstein:
PROFESSION HACKER

Les CASINOS sous la MENACE !

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

EXCLUSIF
UN POSTER
EN CADEAU!

BELUX : 2,3€ - CH : 4,00 FS \$ CAN : 3,25 - DOM : 2,45€

T 02736 5 - F: 2,00 € - RD



Editorial

VOTRE IP A L'ABORDAGE !

Internaute, notre identité ne nous appartient plus...

DoS, masquage d'URL, les attaques à distance menées à l'encontre de nos sites, de nos serveurs et de nos systèmes par de petits malins en soif de pouvoir et de gros sous pullulent. Ajoutons à tout cela les diverses arnaques à la carte bleue, dépouillés que nous sommes après un simple achat en ligne, dit " sécurisé ", il est clair que notre identité n'est plus préservée sur la toile ! L'accès aux informations personnelles, notamment par le biais du " phishing ", ne garantit plus notre sécurité sur le net. Bon. Vous pouvez quand même décompresser :

vos petits HNM vous met en garde contre les atteintes à la vie privée et vous donne même quelques astuces pour ne plus vous laisser avoir sur le Web !

A l'heure où les hackers sont légion, Hacker News Magazine a décidé de se faire l'avocat du diable en vous proposant le portrait d'Emmanuel Goldstein, pirate professionnel, philosophe militant du hacking, au travers de son parcours semé d'embûches. On s'attendrait presque dites donc ! Bon, il faut dire aussi qu'on le cherche, le hackage, en faisant tout passer par l'IP de notre ordi... Peer-to-peer, communications par VOIP, développement de l'IP fixe sur nos connexions Internet, notamment à cause du dégroupage, autant de perches lancées aux pirates pour s'emparer de nos systèmes... Il en

est un autre, bien pire, qui veille aussi au grain et nous observe en douce... Bien plus assidûment. Son nom : le gouvernement. Et oui. Espionnage des connexions des particuliers, dispersion de faux fichiers espions ou même moralisateurs (cf. Ariel Wizman, nldr, lol) sur les réseaux P2P, perquisitions massives aux domiciles des internautes, le règne de la peur s'instaure, celui de la répression guette. Prenez vos bécanes à votre cou, car Big Brother vous observe.

contact@hackernewsmag.com

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

Hacker News Magazine

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

Contact France:

4Ever Paris
35 rue Emile Zola
92150 Suresnes
Tel : 01 41 44 38 70
Fax : 01 45 06 24 19

Ont collaboré à ce numéro:

Anthony Papalia, Grégory Peron,
David Come, Gualtiero, Sergej

Maquette : NoviMedia LLC & OOO

Imprimerie : Roto3 (Italie)

Print : Roto3 (Italie)

Via Turbigo 11/B, CASTANO PRIMO

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 4Ever**

Directeur de la publication

Luca Sprea

Editeur :

4ever S.r.l.

51 via Torino - 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 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.



près de trois semaines provoquant ainsi des préjudices incalculables.

Lille finit par capituler et paie. Il peut désormais travailler mais verse chaque mois une rançon sur un compte lituanien par le biais d'un paiement Western Union.

Depuis, la police australienne est sur les traces des malfaiteurs, avec le concours de différentes forces de l'ordre européennes. Lorsqu'elles les retrouveront, sans doute s'agira-t-il d'une belle prise, car le blocage d'un site pendant trois semaines nécessite une belle armée de zombies.

Des ordinateurs manipulés à leur insu...

Les zombies sont, dans le jargon, les ordinateurs qui servent à l'attaque. Ils sont des milliers, possédés pour la plupart par des citoyens ignorants ou des sociétés employant de piètres administrateurs réseau. Le pirate s'en empare à l'aide d'un vers et peut lancer l'attaque lorsqu'il le souhaite. Selon certaines estimations, 1 % des ordinateurs reliés au Net seraient compromis. Ainsi votre ordinateur est peut-être utilisé à cet instant précis pour lancer une attaque, en même temps que mille ou dix mille autres. Dix mille zombies, c'est une belle armée qui peut rapporter à son chef quelques milliers d'euros.

Les casinos en ligne sont les nouvelles cibles du chantage informatique. Ils gagnent un tas d'argent, dépendent totalement du web, leurs propriétaires les ouvrent dans des paradis fiscaux sans impôt mais où il est très difficile d'obtenir la collaboration de la police.

Actuellement dans l'ensemble, l'éternel jeu du gendarme et du voleur, tourne à l'avantage de ce dernier. Espérons que la tendance s'inverse, avant de se retrouver aux prises avec des bandes d'escrocs à deux sous qui menacent les sites des simples particuliers..

ZOMBI TOI MEME !

Par zombi, on entend un ordinateur infecté par un worm ou un trojan, exploitable à distance pour lancer des attaques DDoS à l'insu de son propriétaire.



NHTCU ET POLICE POSTALE

En Angleterre, la National Hi-Tech Crime Unit (<http://www.nhtcu.org/>) a été créée en 2001, lorsque le gouvernement britannique a pris acte d'un rapport qui dénonçait les risques élevés dus à l'activité des criminels informatiques. Chez nous en revanche, c'est la Police Postale Informatique qui veille sur le cybercrime. Créée dans les années quatre vingt dix, elle dispose de peu de moyen face à la déferlante criminelle qui ne cesse de trouver des parades pour éviter la police.

Denial of Service: l'INPUT Imprévu

L'une des attaques les plus fréquemment utilisées par les script kiddies ou les lamers, en raison de sa simplicité d'exécution, est sans aucun doute le DoS (denial of service; refus de service), c'est-à-dire une attaque destinée à créer un crash momentané du système cible ou de l'application prise dans sa ligne de mire. Les méthodes permettant de lancer une attaque sont nombreuses et l'une des plus exploitées est "l'input imprévu". Voyons comment cela fonctionne.

Le Web et ses applications

Étudions donc le problème dans l'optique Internet. Imaginons un instant un site Web proposant un quelconque module HTML d'enregistrement, lequel doit donner la possibilité à l'utilisateur de choisir uniquement entre les options proposées.

Voici un exemple:

```
<FORM ACTION="processus.cgi"
METHOD="GET">
<SELECT NAME="choix">
<OPTION VALUE="hn">H4ck3r News
<OPTION VALUE="tm">H4ck3r Magazine
<OPTION VALUE="prhack">Prh4ck
</SELECT>
</FORM>
```

Si nous choisissons par exemple le magazine Hacker News, le browser enverrait alors l'URL suivante:

```
"processus.cgi?hn"
```

Notre meilleure défense passe par la connaissance. La première étape consiste donc à comprendre comment fonctionnent toutes ces attaques lancées contre nos serveurs, afin d'en améliorer la sécurité.





DES MAGASINS

150 ARRESTATIONS POUR DDOS

De nombreux crackers américains se sont fait arrêter après avoir lancé plusieurs attaques DDoS (distributed denial of service). Certains étaient même payés par des sociétés qui, par voie télématique, voulaient mettre hors d'état de nuire la concurrence. Mais aujourd'hui, la principale accusée est la mafia lituanienne, la plus dangereuse dans cette utilisation criminelle du réseau, qui fait du chantage aux grands providers télématiques, dont les services peuvent être rendus inaccessibles suite à d'importantes attaques DDoS s'ils ne paient pas la "rançon" exigée.



mais personne ne nous empêche d'envoyer manuellement cette autre URL :

```
"processus.cgi?script%20huddies".
```

Si l'application qui gère le module (en l'occurrence le script CGI processus) s'appuyait sur le fait que le module limite apparemment son choix avec la construction SELECT, et si elle n'était pas programmée pour gérer les données superflues, elle pourrait alors se fermer avec un beau message d'erreur, empêchant ainsi le bon fonctionnement du module pour d'autres utilisateurs.

Les plus gros sites prennent bien évidemment de nombreuses précautions vis-à-vis du module et du programme qui les gère, mais un site plus petit pourrait être exposé à une telle attaque.

Il est donc nécessaire de toujours filtrer les données en input, même si celles-ci se limitent apparemment à des options proposées par le code HTML.

Masquage

Autre aspect intéressant, même si on ne peut pas le considérer comme une véritable attaque DoS: le masquage des URL par le biais de cryptages hexadécimaux ou standards de type UTF8/UNICODE, supportés par presque tous les serveurs.

Si nous passons à un proxy la demande du répertoire /cgi-bin/ avec le fichier d'Unix phf par le biais d'une URL de ce type:

```
http://dommo.com/cgi-bin/phf
```

le browser nous répond généralement par un CGI error ou une erreur 403, pour nous dire que nous ne sommes pas autorisés à accéder au répertoire demandé. Ceci du fait que de nombreux sites bloquent les URL contenant des chaînes du type /cgi-bin/. Mais si nous envoyons la demande de cette façon par Telnet:

```
/%63%67%69%2d%62%69%6e /phf
```

le proxy convertira alors la chaîne hexadécimale en caractères ASCII, en ouvrant le répertoire demandé, en l'occurrence /cgi-bin/phf, mais la demande passée n'est pas exactement identique à celle-ci:

```
http://dommo.com/cgi-bin/phf.
```

En admettant maintenant que le proxy

ait Microsoft IIS sur Windows NT et que nous voulions ouvrir le shell des commandes MS-DOS, nous pourrions lui faire une demande du type:

```
/cgi-bin/.%c0%af.%c0%af.%c0%af.%c0%af/winnt/system32/cmd.exe
```

qui est une chaîne codifiée avec les symboles d'échappement UTF8/UNICODE, semblable à

```
/cgi-bin/../../../../winnt/system32/cmd.exe
```

qui remonte le fichier système de l'unité root vers le dossier où est présent le shell de MS-DOS, à savoir

```
cmd.exe.
```

Qu'avons-nous appris?

L'attaque DoS est une attaque face à laquelle bon nombre de sites peuvent être vulnérables, et qui entraîne une indisponibilité temporaire du site ou de l'une de ses applications auxquelles les autres utilisateurs ne peuvent plus avoir accès.

Si nous ne prenons pas de précautions de filtrage sur les modules d'introduction des données de nos sites, nous serons alors extrêmement vulnérables face aux attaques de ce type.

Si nous ne prenons pas de mesures, avec des techniques similaires prévoyant l'introduction manuelle de chaînes dans

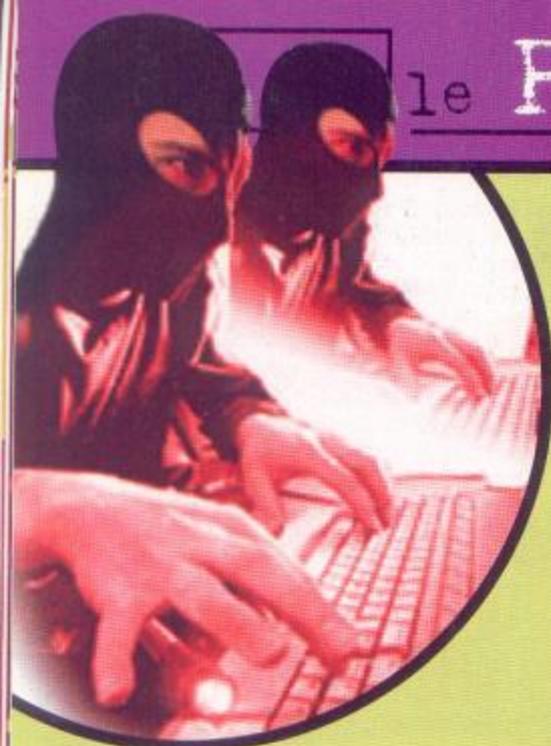
des formats autres que le format ASCII, certaines personnes malintentionnées pourraient alors remonter facilement aux répertoires contenant les fichiers système de notre proxy.



Lord Anonymous
lordanonymous@altervista.org

À L'ASSAUT DES LIENS

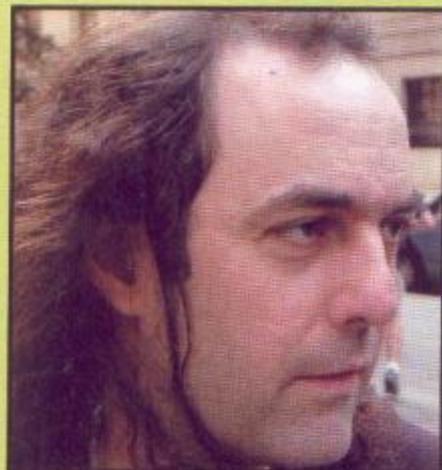
Vous pouvez trouver un forum de discussion sur les sujets que nous avons brièvement présentés ici à l'adresse <http://lordanonymous.altervista.org>, avec un sujet supplémentaire: l'input imprévu dans les query SQL. Un autre site avec plusieurs liens sur des documents concernant ce sujet: www.denialinfo.com/



M. 2600

EMMANUEL

*Sa spécialité:
hacker information. Mais
si vous entendez un
sifflement de 2600 hertz,
c'est sûrement
lui...*

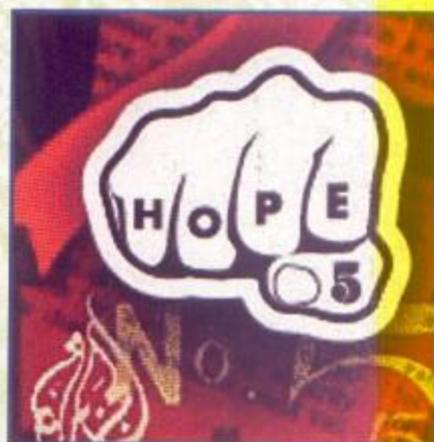


New York City, 31 août 2004, près d'Union Square, un groupe de manifestants bruyants proteste contre la convention républicaine. En période d'élections, comme tout le monde le sait, tout peut arriver: d'ailleurs, une impitoyable caméra vidéo suspendue à l'angle de la 16ème rue enregistre l'arrivée de la police. 150 manifestants sont embarqués et emmenés au poste. La manifestation se disperse parmi les cris des participants en fuite. Rares sont les quotidiens ayant relaté ces faits. Une opération des plus anodines... Mais à la rédaction de "2600 - The Hacker Quarterly", tout le monde est en émoi. Parmi toutes les personnes embarquées par les policiers, se trouve également leur fondateur historique: Eric Corley, plus connu sous le nom d'Emmanuel Goldstein. Les derniers bulletins d'information annoncent sa libération après 32 heures d'incarcération et de contrôles. Cela n'a pas dû être facile... étant donné ses antécédents.

Au début des années 90, la revue et son fondateur étaient en effet dans la ligne de mire d'un tribunal, accusés de "distribution illégale de softwares" par la MPAA, la puissante association américaine pour les droits cinématographiques. Le chef d'accusation retenu contre Goldstein était d'avoir permis la distribution du DeCSS, la célèbre clé pour le décodage des DVD. Convaincu du bien-fondé de sa cause, il sera pourtant condamné par la cour du district de New York, juste après la mi-août 2000. Goldstein dut retirer le software de son serveur et payer les frais de justice.

Hacker lettré porté sur la théorie

Après avoir grandi à Long Island, New York, il se passionne immédiatement pour la technologie, au point d'en être envoûté comme devant une très belle femme nue, mais intouchable, sur le Web. À cette époque, il vit de hacking



HOPE, l'Hacker

sans mettre les mains dans le cambouis: il le théorise sans se salir. Mais est-ce réellement sa vraie personnalité? S'étant épris de la fréquence radio et après être devenu acteur radio-phonique, il devient protagoniste de la radio de son collège lorsqu'il s'inscrit à la State University de New York. Parallèlement à cette culture hacker, se développait et se répandait très rapidement, ces mêmes années, la culture yippie avec des personnages marquants comme Abbie Hoffman. Une figure qui constituera réellement un point de référence important pour Goldstein. Toujours plus porté sur la théorie que la pratique (du moins en apparence), Emmanuel deviendra peu après l'un des noms les plus appréciés et respectés du milieu hacking, pour son esprit créatif, ses nombreuses campagnes pro hacker et ses informations constantes dans les différentes revues avec lesquelles il collaborait.

Eric fonde la revue hacker par excellence: "2600 - The Hacker Quarterly". Spécialisée dans le phreaking et l'ingénierie sociale, le nom de la revue dérivera de la fréquence de la tonalité émise par les téléphones pour les connexions interurbaines aux États-Unis: 2600 hertz.

GOLDSTEIN



On Planet Earth

Un groupe de 60 000

La revue s'impose aussitôt et s'octroie une belle part du " marché underground ": environ 60 000 fidèles lecteurs issus du monde entier, plus quelques autres curieux occasionnels. Elle fait automatiquement autorité dans le milieu hacker et devient la revue la plus surveillée par les autorités et les tribunaux américains. Cette étroite surveillance s'explique également par le fait, qu'après sa création, 2600 suit de près les événements les plus importants liés au hacking et lance de grandes campagnes contre les autorités. Dès qu'il le peut, Goldstein s'insurge contre les sentences émises par les tribunaux, qu'il considère comme injustes et exagérées. Un rebelle à tout prix? Peut-être, mais il n'avait pas totalement tort de dire la vérité. Pensons au cas de Craig Neidorf, plus connu sous le nom de Knight Lightning. Ce garçon s'était donné beaucoup de mal pour parvenir à rentrer dans les systèmes de la Bell South, y aspirant un beau paquet de données considérées comme des secrets industriels. Comme ce hobby, on le comprend, n'est pas particulièrement bien apprécié de ceux qui investissent des millions de dollars dans ces secrets, il fut arrêté et sévèrement jugé.

Comment cela s'est-il terminé? Il a été acquitté, que nous le croyions ou non, car la revue 2600 démontra que les données dont Knight Lightning s'était emparé à partir des systèmes Bell South pouvaient régulièrement et légalement être achetées pour quelques dollars. Sans doute Knight s'était-il procuré ces informations différemment, mais c'est une autre histoire.

Les derniers combats

Août 1994: 2600 invite tous les adeptes de la revue à participer à la première conférence planétaire des hackers, HOPE. Lors de l'Hacker On Planet Earth, on parle de tous les aspects du hacking, des dernières affaires suivies par la justice, on fait des discours sur les derniers projets, on présente de nouveaux softwares, et des discussions techniques sont lancées, mais on parle surtout du Condor. Kevin Mitnick est en prison et l'HOPE poussera le premier cri " libérons Kevin ". Tout le mouvement hacker suit les participants de cette première conférence. Le 21 janvier 2000, Eric Corley se rend devant la prison où le Condor est finalement relâché quelques minutes plus tard. Goldstein ne résiste pas au micro et, en direct sur " Off the Hook ", une émission devenue célèbre et diffusée par la station de radio WBAI, il parle et fait parler son hôte d'exception qui, en prison, a certainement eu le temps de préparer un beau discours.

Mais les années passent pour tous. L'esprit rebelle de certains s'amenuise et, à l'exception de quelques batailles encore vécues sur le terrain, elles restent aujourd'hui des symboles d'un monde révolu. Mitnick en est d'ailleurs un bel exemple: en costume cravate, le consultant en sécurité est apparu à la quinzième conférence HOPE, où il s'est lancé avec Goldstein dans un extraordinaire show dialectique.

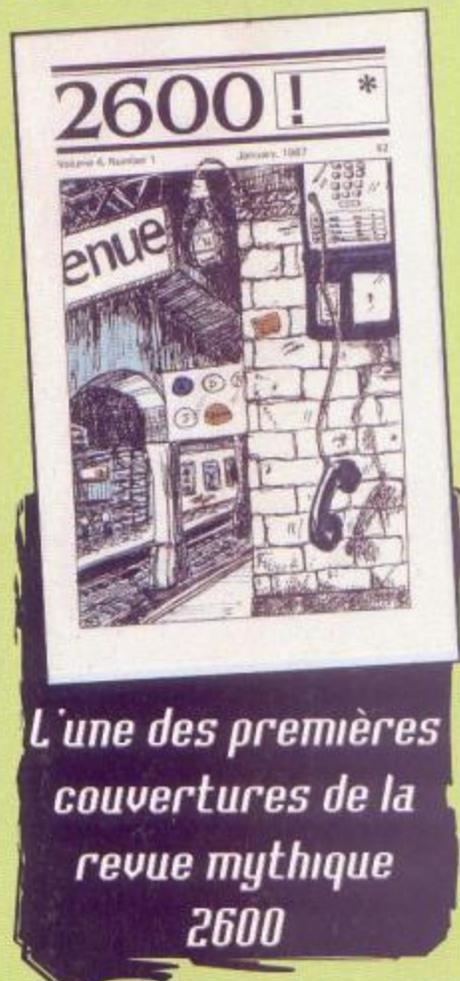
Avec la contribution de
None Sparrow

Orwell, 1984

Goldstein n'est autre que le nom donné par George Orwell au héros de " 1984 ", la figure rebelle, celui qui écrivit " The Book ", Le Livre, qui comportait toutes les hérésies et qui circulait clandestinement un peu partout. Aujourd'hui, il y a encore ceux qui comparent la première figure de Goldstein à celle du diable, ou de Ben-Laden. La discussion reste ouverte...



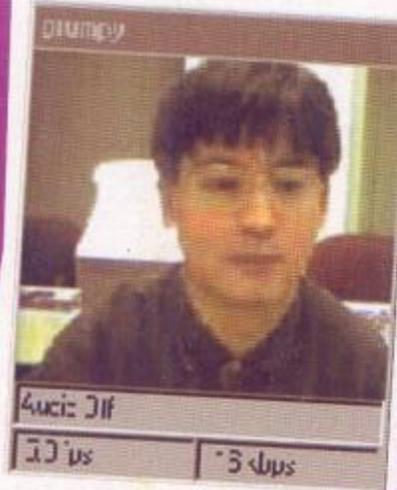
L'auteur de 1984, le créateur de
Big Brother.



L'une des premières
couvertures de la
revue mythique
2600

De la THÉORIE au

De quoi avons-nous besoin pour communiquer en temps réel à travers le réseau IP (Voice over IP) et parler sur Internet comme s'il s'agissait d'une simple ligne téléphonique?



Comme déjà évoqué dans nos numéros précédents, voici la configuration minimale pour communiquer à travers le réseau IP et faire voyager sa voix sur Internet: PC processeur 386 GHz, carte audio full duplex, et bien sûr une connexion Internet. Une configuration de base largement dépassée par n'importe quel ordinateur de moins de cinq ans. Il faut parfois ajouter à cela une carte d'accélération hardware comme PhoneJack ou LineJack de Quicknet (<http://www.quicknet.net/>), capable de compresser l'audio de façon efficace. Mais parlons maintenant un peu des logiciels.

Le système d'exploitation

Pas de problèmes particuliers pour un fonctionnement sous Windows, Mac OS X ou Linux: tous les programmes sont parfaitement compatibles avec ces trois systèmes d'exploitation. On devra, dans le pire des cas, choisir des logiciels spécifiques.

Sous Windows, les logiciels permettant de communiquer par réseau



Vous trouverez ce téléphone Cisco à l'adresse <http://www.cisconetwork.net/html/index.php>. Un téléphone qui vous permettra de communiquer par le biais du réseau IP, et même sans fil si vous le souhaitez!

IP sont nombreux: pour n'en citer que quelques-uns, Netmeeting, Internet Phone, DialPad. Les utilisateurs de cartes Quicknet pourraient également opter pour Internet Switchboard. Vous trouverez bien évidemment tous les logiciels freeware grâce au travail du groupe OpenH323 (<http://www.openh323.org/>).

OpenH323 est incontournable pour Linux. Certains programmes de la gamme, comme Simph323 ou Ohphone, fonctionnent également avec les cartes d'accélération hardware Quicknet.

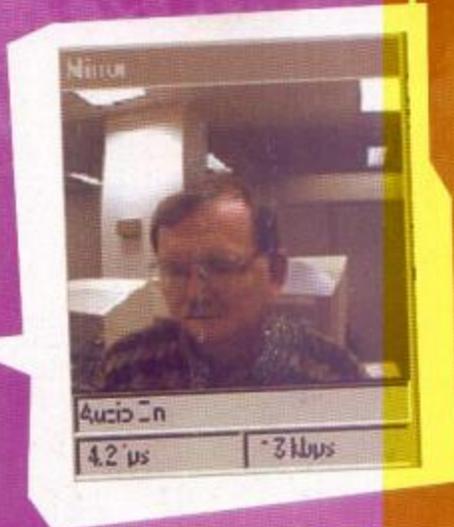
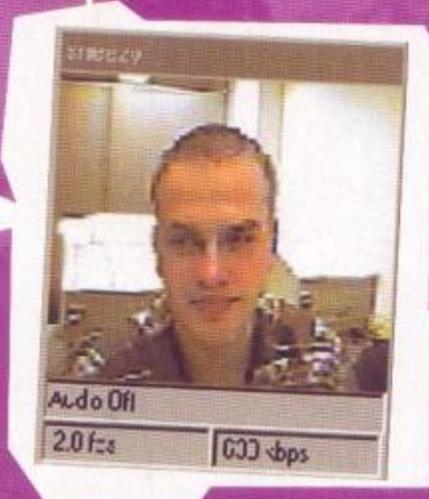
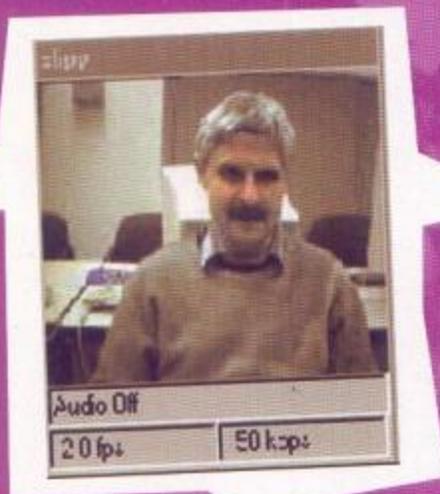
Sur Mac OS X, Apple propose iChat AV (<http://www.apple.com/it/ichat>).



VOIP

PROGRAMMES UTILISANT H.323

Microsoft NetMeeting - <http://www.microsoft.com/windows/netmeeting/>
 Net2Phone - <http://www.net2phone.com/>
 DialPad - <http://www.dialpad.com/>
 Software open source (par exemple GnomeMeeting et Ophone dans le cadre du projet OpenH323 - <http://www.openh323.org/>)



On peut également utiliser tous les programmes qui existent pour Linux. Les logiciels sont parfois prêts au téléchargement (taper <http://xmeeting.sourceforge.net/> ou http://www.ioxperts.com/apps_osXvideo.html), ou nécessitent de remplir un formulaire.

Logiciels gateway

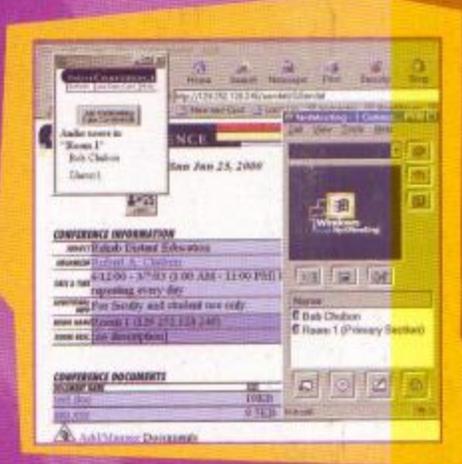
Supposons que nous voulions communiquer sur réseau IP et que nous voulions faire aboutir notre appel, lorsque cela est nécessaire, sur une ligne téléphonique traditionnelle (PSTN, Plain Standard Telephone Network). Nous avons alors besoin d'un logiciel gateway, comme Internet SwitchBoard (<http://www.quicknet.net/>) pour Windows, ou PSTNGw, que l'on peut trouver dans le software Openh323, et qui fonctionne sous Windows, mais aussi sous Linux.

Il nous faudra également un logiciel gatekeeper, c'est-à-dire un logiciel de gestion de l'ensemble du système. OpenH323 met à disposition GNU Gatekeeper, sur <http://www.gnugk.org/>, et Opengatekeeper, pour Linux et Windows, à l'adresse <http://opengatekeeper.sourceforge.net/>.

Dernier software, utile pour la résolution des problèmes:

Phonepatch

(<http://www.equival.com/phonepatch> ou <http://phonepatch.spbbs.com:1084/>), un logiciel capable de contourner les problèmes générés par la présence d'un firewall NAT. Phonepatch permet aux utilisateurs (à l'intérieur ou à l'extérieur du firewall) d'émettre un appel à partir d'une page Web. Lorsque la Web application présente sur la page comprend que le destinataire de l'appel est prêt, il en avise alors la personne qui appelle: il est ensuite possible d'établir la communication. Vous trouverez une application pratique de ce principe à l'adresse <http://phonepatch.spbbs.com:1084/html/internal.html>.



▲ D'un usage très pratique, l'utilisation de la voix sur Internet facilite également la vie des personnes handicapées.

Contrairement à de nombreux logiciels présentés ici, Phonepatch est payant, mais vous pouvez en télécharger une version démo qui vous autorise des conversations de trois minutes maximum.

Dans un prochain numéro, nous vous montrerons comment configurer les cartes pour communiquer en temps réel sur réseau IP.

OÙ APPROFONDIR LA QUESTION?

<http://www.openh323.org/standards.html> la documentation intégrale sur les standards formant H.323

<http://www.cs.columbia.edu/~hgs/rtp/h323.html> toujours la documentation, mais aussi des exemples et des guides rapides

<http://www.itu.int/itu-t/rec/h/> tous les standards de la série H, sur le site ITU

ASTUCES ET SECRETS de WINDOWS



Windows ne finira jamais de nous étonner et de nous donner de nombreuses possibilités d'exercer notre soif de hacking.

Secret n° 1: négatif!

Imaginons que vous venez d'acheter un nouveau PC. Vous êtes courageux et ne voulez pas perdre votre travail effectué jusqu'à présent: ainsi, vous avez transféré tous les dossiers de votre ancien PC vers le nouveau. Y compris un dossier appelé "bureau", dans lequel vous avez placé par commodité tous les éléments qui étaient justement placés sur le bureau de votre ancien ordinateur.

Puis vous replacez correctement ce dossier sur le bureau de votre nouveau PC, de façon à l'avoir immédiatement sous la main. Dommage:

- si vous cliquez pour tenter d'ouvrir des liens de répertoires, et donc sur le symbole (+) indiquant d'autres objets sous le dossier, votre dossier pourrait bien ne plus s'ouvrir;
- le dossier bureau (le vrai, celui du nouvel ordinateur), pourrait être ajouté plusieurs fois;

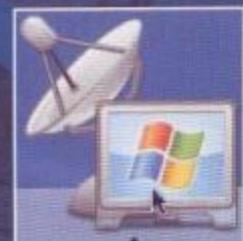
- tous les autres dossiers, ou certains dossiers pris au hasard, pourraient voir leur nom modifié avec d'autres caractères non conformes;

- vous vous trouvez face à une série de messages disant plus ou moins ceci: "F:\Documents and Settings\Administrateur\Bureau\Bureau\Bureau se réfère à un emplacement non disponible. Le dossier pourrait se trouver sur une disquette de cet ordinateur ou sur un réseau. Vérifiez que la disquette est correctement

insérée ou que vous êtes bien connecté à Internet ou au réseau, et essayez de nouveau. Si malgré tout le dossier reste introuvable, l'information pourrait avoir été déplacée à un endroit différent."

Des messages d'erreurs qui peuvent tous apparaître simultanément, un à la fois ou ne pas apparaître du tout, et ce, pendant un certain temps. Que s'est-il passé? C'est simple: vous devez absolument éviter de créer un dossier nommé "bureau" sur le bureau, sous peine de démence précoce de l'explorateur de ressources. Parole de nombreux utilisateurs qui se sont retrouvés dans des situations à la limite de l'absurde, et parole de Microsoft qui nous avertit avec une note technique disponible à l'adresse: <http://support.microsoft.com/default.aspx?scid=kb;en-us;323681&Product=winxp#appliesto>

Astuce n° 2: positive!



Lorsque vous travaillez avec le bureau à distance, vous pouvez commander à l'ordinateur distant de s'éteindre.

Il suffit d'ouvrir le Bloc-Notes ou

un programme analogue, et d'écrire cette ligne d'instructions:

```
[newActiveXObject("Shell.Application")].ShutdownWindows();
```

Il faut ensuite enregistrer le fichier sur le bureau sous le nom RemoteShutdown.js. Un double clic activera alors la coupure du PC.

Astuce n° 3: positive!

Supprimez tout ce que vous pouvez! Vous gagnerez en espace disque et en vitesse de fonctionnement. Voici un dossier à vider sans pitié sous Windows XP: C:\Windows\Prefetch. Un bon nettoyage ne fera absolument aucun mal et les fichiers utiles sont de nouveau recréés automatiquement, jusqu'à la prochaine suppression.

Astuce n° 4: positive!

Éteindre rapidement son PC sous Windows XP? Facile! Il vous suffit de suivre ces quelques étapes:



- cliquez avec le bouton droit n'importe où sur le bureau, faites Nouveau > Raccourci

- dans le parcours, tapez:

```
shutdown -s -t 0
```

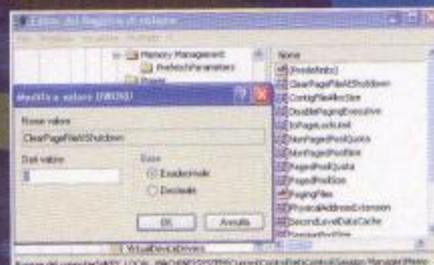
(Pour ne pas se tromper, nous l'écrivons en toutes lettres: shutdown[espace]-s[espace]-t[espace]chiffre zéro)

- cliquez sur Suivant et nommez le raccourci "Eteindre PC" ou comme bon vous semble.

- lorsque vous double-cliquez sur l'icône créée sur le bureau, votre PC ira se coucher!

Secret n° 5: positif!

Les fichiers de paging sous Windows contiennent, comme un cache, les pages des documents Word, les pages explorées du browser, ou encore les informations qui sont ré-allouées par la Ram lorsque celle-ci ne suffit pas ou si de l'espace disque devient nécessaire. Windows est configuré pour ne pas toucher à ce fichier même lorsque vous éteignez votre PC. Mais vous pouvez activer la suppression du fichier de paging chaque fois que vous l'éteignez. Seul problème: lorsque vous éteignez votre PC, le temps de réponse risque d'être plus long. Il suffit de le savoir. Attention toutefois: si vous n'êtes pas maître en la matière, évitez d'utiliser la commande regedit. Vous pourriez créer de sérieux problèmes...



Entrez dans regedit en cliquant sur Démarrer > Exécuter > regedit
Cherchez la ligne

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Sélectionnez

ClearPageFileAtShutdown

À partir de la liste sur la droite, sélectionnez la rubrique Modifier à l'aide du bouton droit. Tapez 1 comme nouvelle valeur et cliquez sur OK. Redémarrez votre ordinateur.

Secret n° 6: négatif!

Imaginons que vous oubliez votre mot de passe d'accès sous Windows XP. Vous pouvez créer une disquette de restauration du mot de passe qui vous permettra de toujours le retrouver lorsque vous devrez en changer. Mais attention! Si vous oubliez au passage votre disquette, n'importe qui pourra alors modifier le mot de passe de votre compte et vous jouer un mauvais tour... avec les conséquences que l'on imagine!

Cliquez sur Démarrer/Paramètres/Panneau de Configuration/Compte Utilisateur et cliquez sur le compte à partir duquel vous souhaitez créer une disquette de restauration. Lorsque vous cliquez sur Restaurer le mot de passe, s'ouvre alors une fenêtre de Création guidée de la disquette de restauration du mot de passe. Insérez une disquette vierge et for-



matée dans le lecteur A: et poursuivez. Pour utiliser la disquette de restauration au lieu d'insérer le mot de passe que l'on suppose perdu, cliquez sur le point d'interrogation et sur la sélection de la disquette de restauration. En suivant la restauration guidée du mot de passe, vous aurez ensuite la possibilité d'en taper un nouveau. Quel que soit le nombre de fois où vous perdrez votre mot de passe, la disquette créée viendra toujours à votre secours!

Le modèle OSI

Comment différents ordinateurs font-ils pour se comprendre? Nous allons tenter une explication qui utilisera des termes comme "niveau physique" ou "niveau de transport". La compréhension de ces termes nous permettra d'y voir un peu plus clair.

Se trouver sur un terrain de football ne signifie pas pour autant pouvoir jouer au foot. Il est nécessaire que les deux équipes connaissent les règles, sachent comment débute le jeu et nomment un arbitre pour calmer les rixes...

Un concept également valable pour nos ordinateurs. Le fait de posséder une carte réseau ne signifie pas pour autant que nos deux ordinateurs reliés l'un à l'autre parviendront à communiquer. Qui plus est s'ils utilisent des applications ou systèmes d'exploitation différents. Ils doivent en effet tous deux respecter les mêmes règles.

Les arbitres internationaux - et donc l'organisation de

standardisation ISO - ont alors tenté de mettre tout le monde d'accord en créant un ensemble de règles, à savoir un modèle appelé Open System Interconnection: OSI.

Le modèle nu

OSI est constitué de sept couches ; chacune possède une fonction spécifique et communique avec le niveau supérieur et inférieur. Plus on baisse de niveau et plus la communication devient primitive. Le premier niveau est le niveau physique, celui des câbles ou des systèmes de transport utilisés pour le transfert des données. Le niveau le plus noble, celui situé au septième étage, est en revanche entièrement destiné à communiquer avec les applications que nous utilisons. Au milieu, on trouve par exemple le chiffrement et toutes les autres opérations que nous voulons effectuer. Le principe de base est que chaque niveau effectue des opérations qui n'exigent aucun changement dans les niveaux supérieurs et inférieurs. En divisant le problème de la communication entre deux ordinateurs, on fait ainsi en sorte de les rendre plus maniables. Il suffit d'influer sur le bon niveau et uniquement sur celui-ci, et le tour est joué!

C'est un peu comme si, par exemple, nous pouvions transmettre nos e-mails par câble ADSL, par fibre optique ou par le biais d'un modem, sans devoir changer de programme.

On comprend mieux en observant! Voyons concrètement ce qui se passe.

OSI CONTRE TCP

Où se situent les protocoles comme le TCP (transmit control protocol) et l'IP (Internet protocol) dans ce palais à sept étages OSI?

Ce schéma vous montre les correspondances. Les attaques DoS à base de ping, par exemple, concernent le niveau trois (lire l'article D.o.S. Partie 1a - PING DE LA MORT, avril 2003, www.hackermag.com). Les exploits qui en revanche concernent le TCP sont placés au niveau quatre.

HACKER JOURNAL

▲ La transmission débute au niveau 1. Nous devons envoyer le message "Hacker Journal" par le biais d'une application quelconque, par mail, par exemple.

UNE TOUTE NOUVELLE VERSION D'EXPLORER EN... 2006 !

Microsoft a annoncé ne pas avoir l'intention de lancer de nouvelle version d'Internet Explorer avant l'année 2006. Le navigateur, dont l'efficacité est depuis peu critiquée à la suite de la détection de plusieurs failles, souffre également d'une



concurrence alimentée par l'émergence des navigateurs gratuits et open source, tels que Firefox de Mozilla. Toutefois, aucune mise à jour ne sera proposée. Seule solution de secours en attendant la prochaine version : les patches de sécurité. Un bien maigre avant-goût.

WIZMAN MORALISE, LE NET LE RIDICULISE!



Ariel Wizman, animateur star de Canal+ et DJ à ses heures, s'est pris la honte sur Internet. Peu avant Noël, il avait prêté sa voix à un message destiné à lutter contre le téléchargement illégal de fichiers sur le

net, message caché dans un faux fichier musical et diffusé sur des services tels que Kazaa avec la participation des divers FAI... Seulement quelques heures après le lancement de cette campagne anti-piratage, le message a été détourné par des internautes, le tout à la sauce caustique sur un lit de ridicule. Un email retransmis massivement invitait les internautes à "utiliser les samples de cette campagne pour réaliser une compilation 100 % artistique". Le pauvre Ariel a pu entendre sa voix remixée avec des samples et des extraits de chansons divers. Le principal intéressé s'est dit quelque peu "mal à l'aise" vis-à-vis du pastiche, il ne souhaitait apparemment pas se

poser comme "le fer de lance contre le piratage"... Comment transformer un émissaire en bouc émissaire en trois clics !

BILL GATES VEUT FAIRE JOUJOU AVEC LE DIVERTISSEMENT

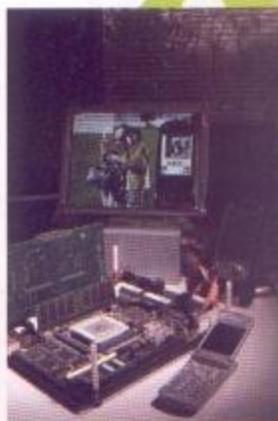
Bill Gates, monsieur monopole logiciels et système d'exploitation, a déclaré début janvier avoir prévu plusieurs alliances qui devraient permettre à Microsoft, son rejeton tout-puissant, de partir à la conquête du marché du divertissement.

Ceci comprendrait entre autres la musique, la photo et les jeux. Mr Gates a également exprimé son désir de développer l'activité de sa compagnie en

direction de la communication numérique. Il a non seulement passé un accord avec le réseau de télévision MTV, mais se serait aussi rapproché de l'opérateur téléphonique Bellsouth. Bill Gates aurait même laissé entendre qu'un partenariat avec Sony serait envisagé, dans une interview accordée au Wall Street Journal. Microsoft pourrait ainsi produire de la musique ainsi que des émissions de télévision qui seraient diffusées sur des supports nombreux et variés, notamment la télévision, les ordinateurs de poche, les baladeurs, les consoles de jeu et même les téléphones, évidemment avec le soutien technique de l'ensemble des logiciels estampillés Microsoft.

GLOBAL INTERFACE VEILLE SUR LES MOBILES

Global Interface, le spécialiste de la gestion de contenus électroniques sécurisés, s'apprête à distribuer une version pour les mobiles de ses logiciels Content Tracker et Content Secure intégrant la norme OMA (Open Mobile Alliance). La téléphonie mobile repré-



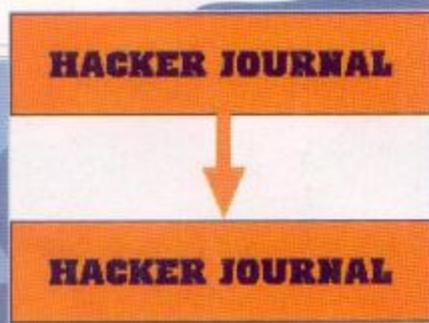
sente un marché juteux, avec des appareils de plus en plus sophistiqués et des réseaux à la couverture internationale. De ce fait, les fournisseurs d'in-

formations souhaitent développer leur activité en terme de texte, musique et vidéo tout en protégeant leurs produits voient dans cette opportunité une véritable mine d'or. Grâce à sa version mobile, Content Tracker permet une traçabilité des fichiers consultés en Wap notamment. Ce dernier ainsi que Content Secure Mobile vont permettre d'ouvrir un passage vers un autre mode d'échange de fichiers musicaux et iconographiques, par le biais du support mobile. Global Interface fournira quant à lui une solution de protection des données et de contenu qui devrait permettre un véritable essor de cette technologie.

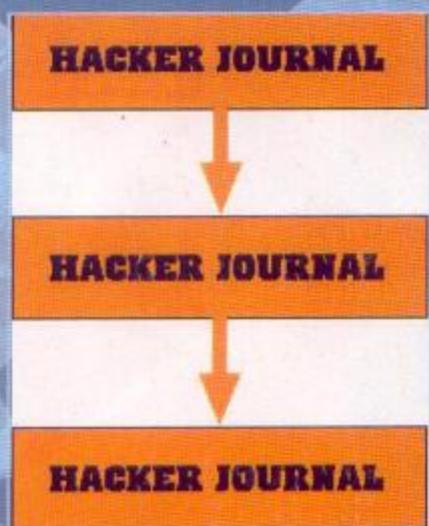
FIREFOX VICTIME DE SON SUCCÈS ?

Le navigateur open source et gratuit Firefox présenterait une vulnérabilité mineure située au sein de la boîte de dialogue apparaissant consécutivement au téléchargement d'un fichier depuis le navigateur lui-même. Les risques encourus sont les suivants : un hacker aurait la possibilité de remplacer un fichier par un virus qui serait transféré sans faire attention. La Mozilla Foundation, développeur de Firefox, a assuré que la faille serait comblée dans une prochaine mise à jour du logiciel.

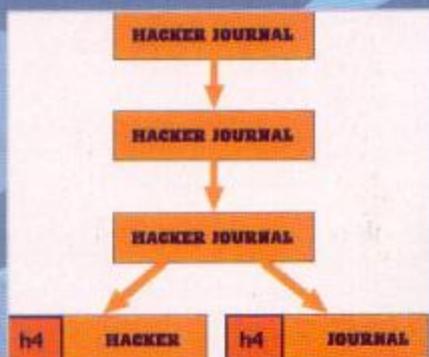




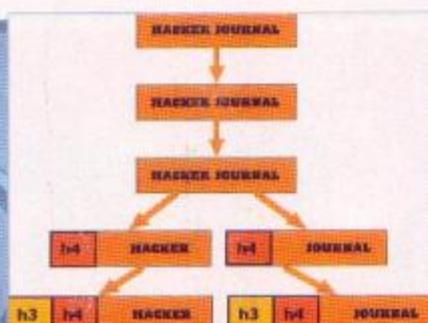
▲ Le message est préparé par le niveau 6 pour être accepté par les niveaux inférieurs. C'est à ce niveau que sont effectués la compression ou le chiffrage.



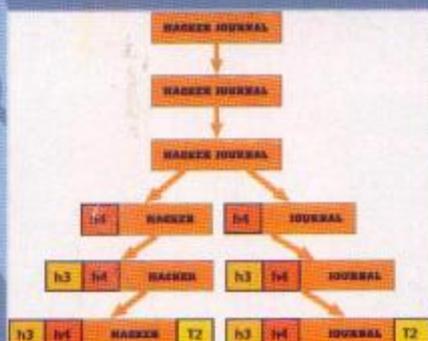
▲ Pratiquement aucun changement significatif. Le niveau 5 règle principalement le flux de données.



▲ Nous sommes toujours dans l'ordinateur qui est en train de transmettre. Au niveau 4, les données sont divisées en paquets plus simples, tandis qu'un nom est attribué à chaque paquet. Les noms comprennent des nombres séquentiels et d'autres informations de contrôle.



▲ Niveau 3: nous nous rapprochons rapidement de la transmission proprement dite des paquets. C'est ici qu'est ajouté un autre nom qui servira au paquet pour être acheminé sur le parcours de destination.



▲ Nous sommes prêts: une queue est accrochée pour adapter les paquets au système qui transportera effectivement les données. Au niveau inférieur, les paquets seront déjà sur un dispositif physique qui devra les transporter, qu'il s'agisse de la micro-onde d'un système Wifi ou du câble d'un réseau Ethernet.



▲ Le message parvient à l'ordinateur du réseau auquel nous sommes connectés. Cet ordinateur vérifie que le message lui est bien destiné. Ce n'est pas le cas: il passe donc le message au niveau 2.



▲ Le niveau 2 le renvoie au niveau physique pour qu'il poursuive sa course vers la machine de destination.



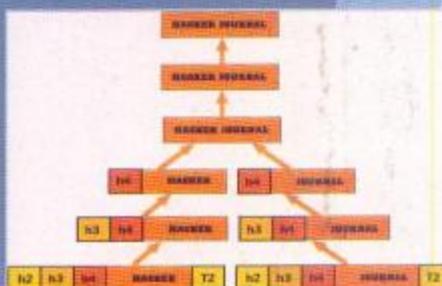
▲ Nous avons finalement reçu le paquet. Le premier nom et la queue sont supprimés. Le paquet est maintenant prêt pour être transféré au niveau 3, de réseau.



▲ Le système contrôle que le paquet est bien adressé à cet ordinateur, puis ce dernier est transféré au niveau 4, le niveau de transport.



▲ Avant de le transférer au niveau 5, le nom est supprimé. Les paquets qui formaient ensemble le message complet sont préparés pour être de nouveau réunis.



▲ Reconstitué au niveau 5, notre message est déchiffré, décompressé et reformaté correctement pour reprendre son aspect d'origine. Les noms et queues ont été supprimés et l'application qui le reçoit peut le mettre au clair. Après un long trajet exténuant, notre e-mail est bel et bien arrivé dans ce réseau qui utilise le standard ISO/OSI.

433

exemples dans

UTILISER LE CARRÉ

Cherchons à l'intérieur de chaque exemple des langages décrits pour apprendre immédiatement beaucoup de choses et pour acquérir une bonne expérience en programmation. Voici, par exemple, le calcul du carré d'un chiffre entre 1 et 10 avec le langage Oz/Mozart, fonctionnel :

```
local ShowIt T in
proc (ShowIt T)
(Show T^T)
end
(For 1 10 1 ShowIt)
end
```

ed eccolo in C#, procedurale

```
using System;
class Squares1 {
static void Main() {
for (int i=1; i<=10; i++) {
Console.WriteLine("{0} ", i*i);
}
}
}
```

e anche in JavaScript

```
<html>
<head>
<title>Javascript Squares</title>
</head>
<body>
<script>
for (var i = 1; i <= 10; ++i)
{
document.write( Math.pow(i, i) + "<br>" );
}
</script>
</body>
</html>
```

ou bien en J

```
*>.i.10
```

C'est bien, n'est-ce pas ?



Dans le monde, les choses fonctionnent de la même façon. Ici, chez nous, nous disons "manger" en français, mais si nous entendons "bouffer", ou "casser la croûte", nous savons que tous ces mots ou expressions ont le même sens, mais dans des registres de langue différents...

En somme, nous pouvons tous être de nationalité française et exprimer les choses de plusieurs façons différentes. Ou bien nous pouvons dire la même chose en anglais, en italien, en allemand sans aucun problème. Le résultat est exactement identique, tandis que la façon de le dire ne l'est pas.

Sommes-nous attachés aux procédures ou plutôt fonctionnels ?

Nous pouvons parler comme nous mangeons. Par exemple, nous pouvons dire à notre sœur, à notre frère ou à

notre mère : "prends une casserole, mets de l'eau et un peu de sel, allume le gaz et lorsque l'eau bout, jette les pâtes, attends dix minutes et fais-les égoutter". Nous décrivons ici une procédure qui nous permet d'arriver au résultat qui est celui de manger.

Ou bien nous pouvons tout simplement crier "manger !" et notre sœur, notre frère, ou notre mère comprendront certainement : ils prépareraient l'eau, le sel, les pâtes... le résultat serait le même. Et voilà, c'est ce que les experts appellent plus ou moins un langage fonctionnel. Cela consiste à dire ce qu'il y a à faire, et ensuite la tâche est effectuée.

Nous sommes donc fonctionnels

Avec les ordinateurs, c'est la même chose, mais contrairement à nos sœurs, lorsque nous disons "fais ceci et fais cela", ils sont tellement idiots qu'ils font réellement ce qu'on leur demande.

Si nous essayons de dresser la liste de tous les langages de programmation existants, nous obtenons au moins cinq cents idiomes qui permettent de dire à l'ordinateur ce qu'il doit faire. Certains en ont regroupé un certain nombre. C'est une occasion unique pour apprendre.

langues différentes

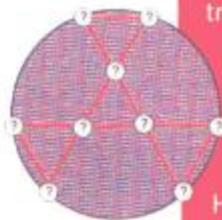
CYBERÉNIGME LOGICIELLE !

Ce n'est certainement pas une véritable cyberénigme qui ressemble à celles que l'on a l'habitude de trouver en dernière page. Mais elle s'en approche... Nous devons classer les chiffres de 1 à 9 en remplaçant les points des questions, de façon à ce que la somme de chaque triangle soit égale à 15 et que la somme de tous les chiffres sur la circonférence soit de 30. Il ne peut pas y avoir deux chiffres identiques.

Solution en Prolog :

```
solve(A, B, C, D, E, F, G, H, I) :-
```

```
{
  between(1,9,A),
  between(1,9,B), B \= A,
  between(1,9,C), C \= B, C \= A,
  between(1,9,D), D \= C, D \= B, D \= A,
  between(1,9,E), E \= D, E \= C, E \= B, E \= A,
  between(1,9,F), F \= E, F \= D, F \= C, F \= B, F \= A,
  between(1,9,G), G \= F, G \= E, G \= D, G \= C, G \= B, G \= A,
  between(1,9,H), H \= G, H \= F, H \= E, H \= D, H \= C, H \= B, H \= A,
  between(1,9,I), I \= H, I \= G, I \= F, I \= E, I \= D, I \= C, I \= B, I \= A,
  A + B + G = 15,
  C + D + H = 15,
  E + F + I = 15,
  G + H + I = 15,
  A + B + C + D + E + F = 30
}
```



Dans certains cas, il existe également de très nombreux langages procéduraux, qui disent donc à l'ordinateur ce qu'il doit faire, étape après étape. Ce sont les plus connus depuis plusieurs années : du Fortran au Pascal, du Cobol au langage C.

Par contre, nous pouvons faire la connaissance de beaucoup de langages fonctionnels : Haskell, Hope, Moby, Pico, Scheme...



▲ Parler un langage ne veut pas dire obligatoirement utiliser la parole.

trouver le compilateur ou les informations les plus approfondies y est également indiqué.

Un site qui s'exprime dans tous les langages

À l'adresse <http://www.ntecs.de/old-hp/uu9r/lang/html/lang.en.html>, nous trouvons un enchevêtrement de fonctionnalités phénoménales.

Pour chacun des 132 langages examinés, une page les décrit brièvement et reporte les liens des langages similaires. Par exemple, sur la page du langage Cilk, les langages sont indiqués de la même façon C, C#, C++, C-Talk, D, Java, Objective-C, Pike, TOM. De plus, le site de référence qui permet de

Apprendre à partir des exemples

Sur le site en question, on peut voir de brefs listages d'exemples qui nous permettent immédiatement de nous faire une idée sur la syntaxe et sur la structure de chaque langage.

La paire "copier/coller" devient un outil formidable, autant pour les débutants qui souhaitent comprendre quelque chose, que pour ceux qui sont déjà expérimentés, mais en considérant que très probablement ils n'ont jamais entendu parler d'Oz ou de Mozart.

La meilleure façon pour apprendre à rédiger dans un langage déterminé est d'observer comment on crée une routine qui résout des problèmes simples.

Mais nous savons bien qu'il existe différentes façons de "parler" aux ordinateurs. Mais combien y en a-t-il en réalité ? Probablement beaucoup plus, même si certains en ont regroupé 164, en comptant les idiomes d'un même langage.



Skype.

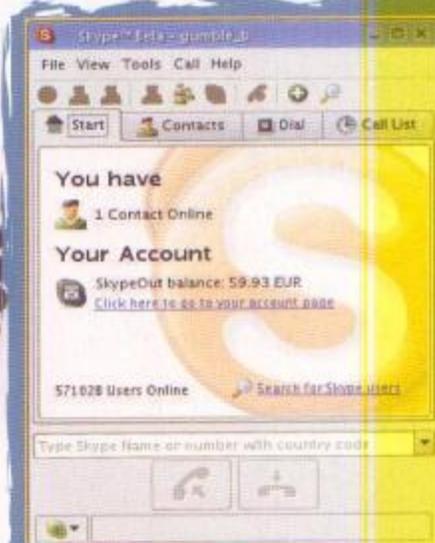
UNE RÉVOLUTION

DANS LA TÉLÉPHONIE

Skype utilise la technologie du P2P, non pas pour échanger des fichiers, mais pour communiquer et - véritable révolution - téléphoner!

Le Web a marqué la première révolution. La seconde s'est caractérisée par l'apparition du peer-to-peer, avec l'effondrement des serveurs centraux (pour paraphraser Asimov) et le pouvoir donné à chaque utilisateur.

La troisième révolution vient à peine de commencer et est plus liée au P2P qu'il n'y paraît. Niklas Zennström et Janus Friis, les créateurs de Kazaa, ont en effet eu une idée géniale: transposer la logique et la puissance du P2P dans le monde



▲ **Légende.** L'interface de Skype est vraiment simple. Avec une carte de crédit à votre disposition, vous pouvez également recharger facilement votre compte pour appeler vers des téléphones fixes. Pour vérifier si la connexion fonctionne, vous pouvez appeler via Skype l'utilisateur échol23, qui ne fait rien d'autre que répéter ce que vous lui dites. Mais s'il y a de l'écho, c'est que ça fonctionne!



LA TÉLÉPHONIE VIA INTERNET SELON SKYPE

	SKYPE	NET2PHONE	MSN M., ICQ, AIM, YAHOO M.	AUTRES CLIENTS VoIP
Aucune configuration particulière	Si	Non	Non	Non
Appels gratuits illimités pour les utilisateurs du même programme	Oui	Non	Oui	Ça dépend
Qualité du son	Comme au téléphone	Pire qu'au téléphone	Pire qu'au téléphone	Pire qu'au téléphone
Communication cryptée pour une plus grande confidentialité	Oui	Non	Non	Non
Aucune publicité	Oui	Non	Non	Ça dépend



de la téléphonie. C'est ainsi qu'est né Skype.

Parler de vive voix avec les utilisateurs Skype du monde entier est totalement gratuit; composer le numéro d'un téléphone fixe, c'est en

revanche payant, même si les tarifs commencent à devenir intéressants. S'il est peu probable que vous utilisiez Skype pour passer des appels locaux à votre copine (ou votre maman) pour lui dire de mettre la table, son utilité est en revanche plus importante lorsqu'il s'agit d'appels nationaux et totale pour les appels internationaux.

Faire voyager sa voix sur Internet n'est certes pas une nouveauté. Mais Skype peut être utilisé sur n'importe quel ordinateur (Windows, Linux, Macintosh et même les ordinateurs de poche!) et ça, par contre, c'est une vraie nouveauté! De plus, et c'est sans doute le point le plus important, Skype fonctionne réellement!! Les autres services sont difficiles à configurer et ne sont pas sans créer quelques problèmes. Mais celui-là, non! L'important étant d'ôter de son esprit

l'idée selon laquelle une simple connexion par modem suffit. Il vous faudra au minimum une connexion ADSL, et une bonne si possible. Mais vous pourrez ensuite profiter pleinement de Skype!

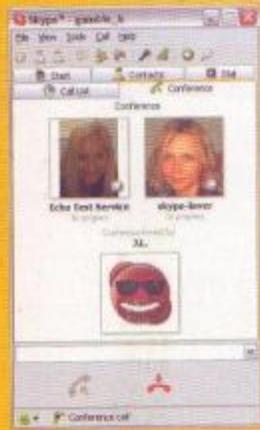
Les secrets du téléphone en P2P

En travaillant sur Kazaa, l'équipe de Skype a parfaitement compris comment exploiter au mieux les ressources du Réseau et faire voyager les données de la façon la plus efficace possible. Ces connaissances, mises au service de la téléphonie, permettent à Skype d'atteindre des taux d'appels et une qualité d'écoute comparables à ceux de la téléphonie conventionnelle (pas la téléphonie portable), qui présente de nombreux défauts, certes; mais 99 fois sur 100, un appel téléphonique arrive à son destinataire, la ligne ne se coupe pas et la conversation est parfaitement comprise. En matière de téléphonie sur Internet, ce sont des objectifs encore lointains, que Skype vient finalement d'atteindre. L'expérience menée sur le P2P a également permis à l'équipe de Skype de faire fonctionner ce système malgré l'activation de NAT et de firewalls, tout en mettant en place un système utilisable immédiatement, sans configuration spécifique.



▲ **Légende.** À l'instar des systèmes de messagerie les plus modernes, Skype permet lui aussi d'associer une photo à un contact.

▼ **Légende.** Jusqu'à quatre personnes peuvent participer à un appel Skype!



SKYPE CONTRE TÉLÉ2

Nous avons comparé les tarifs d'appel téléphonique de Skype avec ceux de Télé2, un opérateur qui peut être considéré comme le moins cher ou parmi les moins chers disponibles. Les prix sont en euros. Les tarifications de connexion sont facturées une seule fois, tandis que les tarifs sont valables pour chaque minute de conversation. Les tarifs de Télé2 sont disponibles à l'adresse <http://www.tele2.fr/telephonie/tarifs/local-national-mobile-international.html>, et ceux de Skype

	SKYPE	ET TÉLÉ2	QUI L'EMPORTE?
Tarif de connexion appels locaux	0	0,0619	Skype
Tarif de connexion appels interurbains	0	0,0775	Skype
Tarif de connexion appels vers portables	0	0,125	Skype
Appels locaux, le jour	0,02	0,011	Télé2
Appels locaux, soir et jours fériés	0,020	0,0058	Télé2
Appels interurbains, le jour	0,02	0,07	Skype
Appels interurbains, soir et jours fériés	0,02	0,02	Égalité
Appels vers portables, le jour	0,288	0,218	Télé2
Appels vers portables, soir et jours fériés	0,288	0,141	Télé2

TÉLÉPHONER AVEC SKYPE: COMBIEN ÇA COÛTE?

Les tarifs pour des appels passés vers certains pays européens et internationaux, en euros par minute. La liste complète se trouve à l'adresse <http://web.skype.com/skypeout/help.pricelist.html>. Les appels de Skype sont toujours arrondis à la minute: parler pendant dix secondes équivaut donc à parler pendant une minute.

Albanie	0,158
Argentine	0,030
Belgique	0,020
Brésil	0,064
Canada	0,020
Chine	0,026
Cuba	0,957
Danemark	0,020
Philippines	0,185
Philippines - Mobile	0,232
Finlande	0,033
France	0,020
Japon	0,031
Grèce	0,031
Groënland	0,537
Inmarsat	Non disponible
Irak	0,347
Irlande	0,020
Israël	0,030
Italie	0,020
Italie - Mobile	0,288
Kenya	0,228
Lybie	0,149
Lituanie	0,105
Maldives	0,269
Malte	0,167
Maroc	0,240
Mexique	0,092
Nouvelle-Zélande	0,020
Hollande	0,020
Pologne	0,030
Royaume-Uni	0,020
République Tchèque	0,027
Roumanie	0,117
Russie	0,060
Espagne	0,020
Suède	0,020
Suisse	0,021
Taiwan	0,025
Thaïlande	0,106
Hongrie	0,039
États-Unis	0,020

Un coût moins élevé, mais un coût tout de même



Si vous avez des parents à l'étranger, un amour lointain ou encore un coup de fil professionnel à passer vers l'international, Skype est alors une alternative sérieuse, prix en main! Vous pouvez retrouver la liste complète

des pays et des tarifs à l'adresse <http://web.skype.com/skypeout/help.pricelist.html>. Lorsqu'aucun tarif national n'est mentionné, Skype vous sera alors facturé 0,017 euro/minute; dans les autres cas, les tarifs varient d'un pays à l'autre. Un appel en Australie vous en coûtera 0,020 euro/minute et 1,009 euro/minute en Guinée-Bissau. Il est également possible d'effectuer des appels vers les téléphones portables, à des tarifs plus élevés bien sûr. Téléphoner vers un portable en Allemagne coûte 0,288 euro/minute. Autre point: les appels locaux. Appeler l'Italie coûte 0,020 euro/minute (comme l'Australie!) et appeler un portable en Italie 0,288 euro/minute (comme l'Allemagne!). Comme on peut le constater sur l'un des tableaux, pour des appels de plus d'une minute, un appel téléphonique conventionnel reste pour l'heure plus adapté. Mais si Skype parvient à prendre racine sur le marché, il y a fort à parier que les choses pourraient bientôt changer.

La concurrence

Skype doit faire face à plusieurs concurrents en matière de téléphonie. L'un d'eux est Net2Phone, mais mis à part le fait qu'il s'adresse plus aux entreprises qu'aux particuliers, ses tarifs sont grosso modo le double de ceux proposés par Skype. Qui plus est, Net2Phone fonctionne uniquement sous Windows, ce qui peut poser un problème, car Windows détient 90 % du marché, mais si votre cousine australienne utilise Linux, c'est alors sur Skype qu'il faudra compter. D'une façon générale, les concurrents de Skype sont moins répandus, proposent

des tarifs plus élevés ou ne fonctionnent pas sur la totalité des ordinateurs. Aucun fabricant de téléphones ne lancerait des modèles qui ne fonctionneraient que dans la quasi-totalité des maisons, pas vrai?

Allo. Skype?

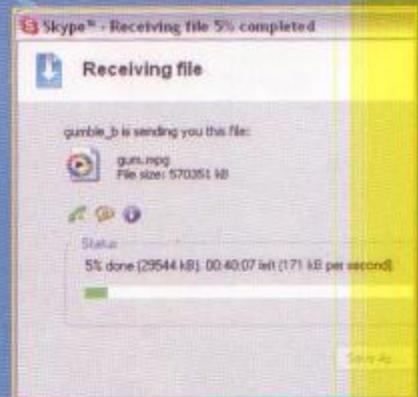
Si vous disposez d'une bonne connexion Internet, alors tenez compte de ce programme. Parler avec les autres Skypistes est totalement gratuit, et téléphoner à l'étranger vous coûtera moins cher. Ce programme est gratuit et fonctionne sous Windows, Mac OS X, Linux et les ordinateurs de poche. Que faut-il de plus pour vous lancer?

Reed Wright
reedwright@mail.net.it

SKYPE CONTRE NET2PHONE

Les prix sont indiqués en euros par minute. Les prix de Net2Phone sont exprimés en dollars et ont donc été convertis avec quelques approximations, ce qui n'altère en rien l'importance des données chiffrées. Vous pouvez trouver les informations précises pour Net2Phone à l'adresse <http://web.net2phone.com/french/consumer/commcenter/>. Celles de Skype se trouvent en revanche à l'adresse <http://web.skype.com/skypeout/help.pricelist.html>.

	SKYPE	NET2PHONE
Canada	0,020	0,040
Philippines	0,185	0,175
Italie	0,020	0,050
Royaume-Uni	0,020	0,040
Espagne	0,020	0,050
États-Unis	0,020	0,040



ENCYCLOPÉDIE du Hacking

Le diffing est une simple attaque prévoyant la confrontation de deux fichiers pour obtenir de précieuses informations. Quels sont les avantages? Si nous avons par exemple à notre disposition un fichier binaire contenant un mot de passe et que nous ne savons pas dans quelle position il se trouve, nous pouvons alors en faire une copie, modifier le mot de passe et le comparer au précédent: on peut alors deviner qu'un byte au minimum ne correspondra pas, et nous aurons ainsi



connaissance de la position du mot de passe.

EXEMPLE

Pour l'exemple, on tentera de modifier l'enregistrement d'un jeu pour obtenir le plus d'or possible. Ouvrons le jeu et notons le nombre de pièces d'or: 7500. Enregistrons maintenant la partie: nous l'appellerons par convention save1.gm1. Ré-ouvrons le jeu et dirigeons-nous vers le château où des objets sont en vente: achetons le moins cher d'entre eux (un squelette). L'or se monte désormais à 7425 pièces. Enregistrons de nouveau la partie sous save2.gm1. Dirigeons-nous vers le dossier des enregistrements et là, ouvrons le prompt de MS-DOS, et avec les commandes 'cd nomdossier', tapons la commande 'fc /b save1.gm1 save2.gm1'. FC est l'utilitaire qui permet de comparer deux fichiers, le paramètre '/b' concerne la comparaison binaire puis les noms des fichiers à comparer.

Voici un output possible:

```
C:\Programme\MightAndMagicII\save>fc /b save1.gm1
save2.gm1
Comparaison en cours des fichiers save1.gm1 e
save2.gm1
000002A2: 31 32
000002C3: 32 FF
00000306: FF 03
00000368: 4C 01
```

```
00003ACE: FF 2F
00003AD3: 00 01
00003AE4: 08 07
```

```
C:\Programme\MightAndMagicII\save>
```

Ouvrons maintenant la calculatrice de Windows et dans le menu "Affichage", choisissons "scientifique". Appuyons sur la touche "Déc" et tapons 7500 (les pièces d'or). Cliquons sur "Hex" et nous obtenons le correspondant hexadécimal, à savoir: 1D4C. En répétant l'opération avec la valeur 7425 (c'est-à-dire le nombre de monnaies disponibles après l'achat du squelette), nous obtenons 1D01. Si l'on regarde les indices, on peut noter la ligne à l'adresse 00000368 dont la valeur est passée de 4C à 01, ce qui correspond exactement aux pièces d'or en hexadécimal. L'étape suivante comporte la modification du fichier. Ouvrons donc, avec un éditeur hexadécimal, le fichier save2.gm1 et modifions l'offset (adresse) 00000368 où se trouve le chiffre 1D01. Modifions ensuite le byte à sa gauche (1D), celui-ci étant le plus significatif: en mettant FF (qui représente le maximum en hexadécimal), on obtient la plus grande quantité d'or possible. Nous pouvons même modifier le byte 01 pour obtenir encore plus d'or, à condition toutefois que le jeu le permette. On pourrait donc aussi parvenir à comprendre le sens des autres bytes trouvés pendant la comparaison avec MS-DOS, mais laissons ce plaisir à l'expérimentation.

Conditions:

Un éditeur hexadécimal quelconque et un jeu de rôle ou d'imagination (dans l'exemple, Heroes of Might and Magic II).

Sécurité

Certains jeux ou programmes pourraient utiliser des techniques comme la compression de fichiers "délicats" et rendre impossible l'exploitation de cette technique. Il s'agit bien évidemment d'un exercice purement expérimental et didactique, car la licence interdit formellement la modification des fichiers source de programmes commerciaux.

ENCYCLOPÉDIE du Hacking

Hash



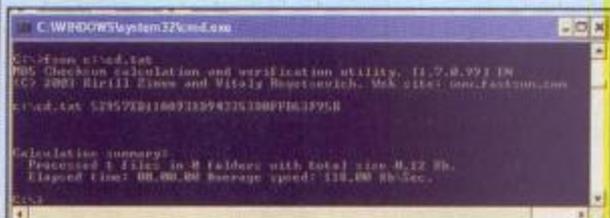
Hash est une opération de chiffage d'un texte entier, qui génère une chaîne de longueur fixe et qui est univoque pour ce message spécifique. Par exemple, une chaîne de 128 bits que l'on peut associer à ce texte

spécifique et à aucun autre. La probabilité d'avoir une autre chaîne identique pour un message différent est inférieure à celle qu'aurait un astéroïde de nous percuter et de supprimer toute vie sur terre... Il est impossible de remonter au message entier par la chaîne de longueur fixe générée : on dit qu'il s'agit d'un système "one-way", à sens unique. C'est une opération utilisée pour créer une sorte d'empreinte digitale d'un texte quelconque, pour que vous puissiez noter toute modification, volontaire ou non. Elle est souvent utilisée lorsque vous téléchargez un fichier, de façon à vérifier que vous avez bien récupéré l'ensemble du fichier ou que personne entre-temps ne l'a remplacé ou endommagé.

EXEMPLE

Fastsum est un programme qui fonctionne par ligne de commande. Par conséquent, après l'avoir téléchargé et installé, rappelez-le en cliquant sur Démarrer > Exécuter > cmd. Sur la ligne de commande, écrivez fsum suivi du parcours du fichier à partir duquel vous souhaitez générer la chaîne MD5. Si vous ne spécifiez pas d'autres paramètres, la chaîne est affichée sur votre écran. Sinon, vous pouvez l'enregistrer dans un fichier ou insérer d'autres paramètres en suivant les instructions du fichier d'Aide que vous ouvrez sur votre browser à partir du répertoire :

file://localhost/c:/Programmi/FastSum/How to use FastSum.htm



Voici quelques célèbres algorithmes d'hashing :

SHA-1

C'est l'algorithme de hash considéré comme le plus sûr, si vous n'avez pas de problème de vitesse de calcul.

MD5

Est un système d'hashing très répandu, même si ce n'est pas la méthode la plus sûre dans l'absolu. Si les données sont vraiment importantes, mieux vaut utiliser SHA-1 qui est inattaquable.

RIPEND

MD4

Algorithmes de hash utilisés avant l'an 2000, désormais peu fiables et dépassés.

Conditions requises

Un programme rapide de génération de contrôle de chaînes hash selon le standard MD5, par exemple

<http://www.fastsum.com/download/fsum-setup.exe>

Security

Esistono strumenti software che ci consentono di controllare un intero sistema dalle possibili intrusioni, calcolando periodicamente una stringa hash per ogni file presente su un disco e quindi confrontando tutte le stringhe con quelle precedenti. Dove ci sono stringhe diverse, c'è stato un cambiamento del file e la traccia del tutto viene mantenuta in un database. L'analisi del database consente di evidenziare i cambiamenti significativi ed eventualmente pericolosi. Il progetto OpenSource Tripware che applica il tutto all'ambiente Linux lo troviamo a www.tripware.org. MD5, per esempio: <http://www.fastsum.com/download/fsum-setup.exe>

LIENS:

Un système rapide de génération de chaînes hash MD5, à ligne de commande : www.fastsum.com

Le projet OpenSource de contrôle de l'intégrité des données par l'intermédiaire de hash : www.tripware.org

La version commerciale et pour Windows du software Tripware : www.tripware.com

Un simple programme de contrôle hash de l'intégrité des fichiers gravés sur CD : www.brandonestaggs.com/filecheckmd5.html



BONNES RUNES: LA REPONSE

POUR LA CYBERENIGME BASEE SUR L'ALPHABET ESOTERIQUE DU SEIGNEUR DES ANNEAUX VOICI LA REPONSE

L'énigme était rédigée dans un italien parfait, mais avec des alphabets runiques. Les phrases étaient les suivantes :

POUR LES HUMAINS: où peut-on trouver ces polices sur le Web?

POUR LES NAINS: comment s'appelle cet alphabet ? Quelle race l'utilise dans le Seigneur des Anneaux ?

POUR LES ELFES: comment s'appelle cet alphabet ? Quelle race l'utilise dans le Seigneur des Anneaux ? Connais-tu un site qui apprend à écrire avec cet alphabet ?

POUR LES PORTEURS DE L'ANNEAU UNIQUE: Comment s'appelle cet alphabet ? Peux-tu redonner l'inscription qui était gravée sur l'anneau ? Sais-tu comment a-t-elle été traduite en italien ? La phrase pour les humains était rédigée clairement. La police s'appelle Ringbearer et se trouve à l'adresse <http://simplythebest.net/fonts/fonts/ringbearer.html>.

La phrase pour les nains disait : comment s'appelle cet alphabet ? Quelle race l'utilise dans le Seigneur des Anneaux ? Les runes sont Cirth, utilisées bien sûr par les Nains selon Tolkien. La police s'appelle Angerthas et se trouve à l'adresse <http://simplythebest.net/fonts/fonts/angerthas.html>. Pour les Elfes : la phrase disait : comment s'appelle cet alphabet ? Quelle race l'utilise dans le Seigneur des Anneaux ? Connais-tu un site qui apprend à écrire avec cet alphabet ? Il s'agit du Tengwar Quenya, utilisé par les Elfes. La police se trouve à l'adresse http://simplythebest.net/fonts/fonts/tengwar_quenya.html, tandis qu'à l'adresse <http://www.sci.fi/~alboin/tengwartutorial.htm>, vous trouverez une

aide en ligne qui vous expliquera comment l'utiliser. La phrase finale, pour les porteurs de l'anneau unique, disait : comment s'appelle cet alphabet ? Peux-tu répéter l'inscription qui était gravée sur l'anneau ? Sais-tu comment elle a été traduite en italien ? L'alphabet est toujours

le Tengwar. L'inscription originale (celle-ci était difficile !) disait : ash nazg durbatulúk, ash nazg gimbatul, ash nazg thrakatulúk agh burzumishi krimpatul. En français, c'est un anneau pour les dresser, un anneau pour les trouver, un anneau pour les saisir et les enchaîner dans le noir. Toutes ces polices sont gratuites et peuvent être utilisées sans problème sur Windows, Linux et Mac OS X.

Les réponses !

PREMIER ARRIVÉ : Gemini Nero !
Suivi de : BufferOverflow (15 ans, félicitations !), Pippo Pizza, [Alex], devilangel666, (Eagle), DarkLink, M@rk01, Surf3r, Fabien Mhu Calzamid, TheGryffin, dottor_p, Rodry, Dominique, Vlad87, Valkiry, Free4life, Silviasilvia et Fcx.

Salut à tous, bravo et... rendez-vous à la prochaine cyber-énigme !

Barg the Gnoll
contact@hackernewsmag.com



AUTRES SITES CONSEILLÉS

Tolkiendil

Le site Tolkiendil vous propose toute une série de fontes, qui vous seront utiles pour recréer des textes tels que les caractères apparaissant sur la Porte Ouest de la Moria ou même ceux de l'Anneau Unique...

Lien téléchargement : <http://www.tolkiendil.com/telec/polices/tengwar.php>



Ambar Eldaron

Envoyer des cartes de vœux en Quenya, ça vous tente ? Et des cours de Sindarin, c'est alléchant non ? Téléchargez en prime sur le site Ambar Eldaron une pléthore de polices de caractères dans la partie Scriptorium.

Lien téléchargement : <http://www.ambar-eldaron.com/scriptorium1.htm>



Les Archives de Gondor

Angerthas, runes, graphie Celte et bien sûr Tengwar, les Archives de Gondor ne laissent rien au hasard. Grâce à ce site, vous deviendrez un véritable scribe elfique !

Lien téléchargement : http://perso.wanadoo.fr/archives_gondor/html/downloads/polices.html



"[...]Je dirais que dans les économies du monde, il y en a aujourd'hui encore plus que jamais qui croient en la propriété intellectuelle. Il y a moins de communistes dans le monde aujourd'hui qu'il n'y en avait avant. Il y a quelques nouvelles sortes de communistes des jours modernes qui veulent se débarrasser pour divers prétextes des incitations faites aux musiciens, aux réalisateurs de films et aux créateurs de logiciels. Ils ne pensent pas que ces incitations devraient exister."

Bill Gates



Microsoft:

Bénéfice 2003: 2,14 milliards de \$

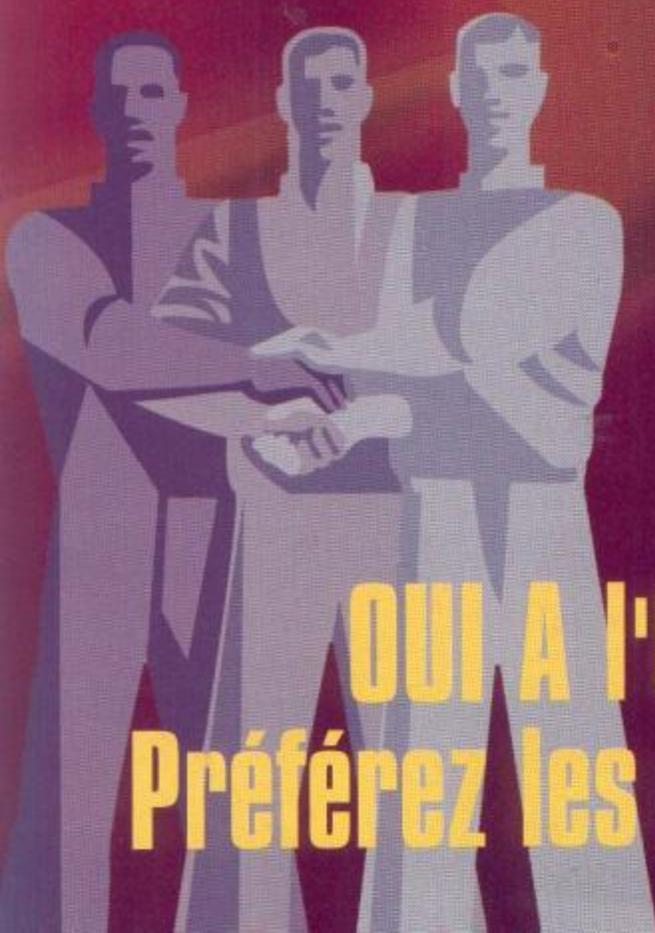
Justice: Condamnations multiples

Bill Gates:

46,6 milliards de \$ de fortune personnelle

Bill Gates et Microsoft ne sont pas si regardants lorsqu'il s'agit de vous vendre leurs logiciels hors de prix.

OUI A L'OPEN SOURCE
Préférez les logiciels gratuits !



ATTAQUE DE POP-UP SOUS COUVERT DE FICHIERS MUSICAUX

De faux fichiers musicaux circulent bel et bien sur les réseaux peer-to-peer, c'est ce qu'a démontré en janvier dernier le magazine américain PC World. Le nom du coupable : Overpeer, appartenant à Loudeye, fournisseur de contenu pour iTunes... Plusieurs utilisateurs se sont rendus compte, en téléchargeant certains

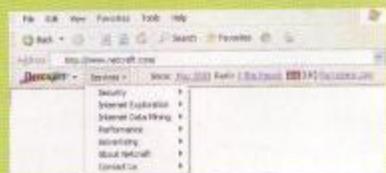
fichiers musicaux, de manière illégale, que certains morceaux au format .wma ne correspondaient non seulement pas à la chanson

téléchargée, mais en plus ces fichiers laissaient place à une série anarchique de pop-up. Ces mêmes pseudo fichiers musicaux tentent de modifier la page de démarrage d'Internet Explorer et de rediriger l'internaute vers l'application "180search assistant" par le biais d'une fenêtre l'incitant à télécharger un certain fichier "lyrics.zip".



UNE BARRE D'OUTILS ANTI "PHISHING" POUR INTERNET EXPLORER

Le spécialiste des solutions d'analyses Netcraft vient de publier gratuitement une barre d'outils destinée à améliorer la sécurité d'Internet Explorer, notamment les versions du navigateur antérieures à la version incluse dans l'update SP2 de XP. Son action va se porter sur le phishing par pop-up, en



résumé, une fenêtre pop-up s'ouvre lors du surf, ayant pour objectif de récupérer des données personnelles de l'internaute. Cette barre d'outils s'ajoute directement à Internet Explorer et va s'atteler à surveiller les sites visités, en temps réel. La barre s'est constituée une base de données grâce aux renseignements de ses utilisateurs. En conséquence, si l'un de ces sites est répertorié, l'accès est bloqué, puis un message d'alerte retentit. Au menu des fonctionnalités de cette barre d'outils, l'affichage d'informations sur le site en question, dont l'identité et la localisation géographique de son hébergeur. Elle est téléchargeable directement sur le site de Netcraft. Attention, elle ne fonctionne pour l'instant qu'avec Internet Explorer et sous Windows 2000 ou XP. Netcraft a cependant précisé qu'il développait une version exploitable pour le navigateur open source Firefox, de Mozilla.

Lien téléchargement : <http://toolbar.netcraft.com/>

MICROSOFT ACCOUCHE D'UN ANTI-SPYWARE

Microsoft, notre ami à tous, a lâché dans l'arène un nouveau fauve, en janvier dernier. Répondant au doux nom d' "Atlanta", ce petit bébé MS est un anti-spyware que beaucoup attendaient. MS testait encore cette version Beta 1 en janvier, avant que l'application ne puisse voir le jour. Sa mise sur le marché est imminente. Basé en grande partie sur le logiciel de Giant Company Software Inc., une société précédemment rachetée par Microsoft, Atlanta Beta 1 est une version

dépoussiérée et améliorée de son aîné. Le logiciel a été conçu pour se débarrasser de certains programmes, provoquant notamment l'affichage de fenêtres pop-up publicitaires sur votre ordi.



NAPSTER CÔTÉ EN BOURSE !

Voici une info un peu hallucinante : Napster, l'ancien bandit du net, celui par qui le scandale arriva dans le monde balbutiant du P2P et du téléchargement illégal de musique, est coté au Nasdaq, l'indice regroupant les principales sociétés technologiques américaines, depuis le mois de janvier. Inscrit sous l'appellation NAPS, il remplace le titre Roxio (ROXI). Napster, interdit en 2001 pour cause de piraterie musicale, avait été racheté en novembre 2002 par Roxio, qui en avait profité pour lancer en 2003 un service tout à fait licite de téléchargement de musique.

HOT NEWS

FUJITSU-SIEMENS TAXÉ À CAUSE DU PIRATAGE

VG Wort, une association allemande a réussi, par décision de justice, à obliger Fujitsu-Siemens, le plus gros fabricant de PC du pays, à verser douze euros par ordinateur vendu. La raison invoquée à cette amarque : la compensation des pertes consécutives au piratage. Fujitsu-Siemens compte évidemment faire appel de cette décision. Il est vrai qu'en France les supports vierges sont déjà taxés... cela s'appliquerait-il aux constructeurs français dans un proche futur ?

ENCORE UN ÉCHEC POUR LA RIAA

La Recording Industry Association of America, association interprofessionnelle superpuissante défendant les intérêts de l'industrie du disque américaine, a été déboutée en justice par une seconde cour d'appel américaine, après que la RIAA a fait la demande de révélation d'identité des abonnés internautes suspectés de piratage. Une première cour d'appel du district de Columbia avait déjà rejeté une demande similaire de la part de la RIAA en décembre 2003. Un second échec cuisant pour l'association à seulement quelques semaines d'intervalle !



SKYPE VEUT IMPLÉMENTER UN SYSTÈME DE MESSAGERIE VOCALE PAYANTE

téléphonie Gratuite par Internet qui fonctionne vrai

Skype v1.1

© 2002 Skype Technologies S.A.
Registered in Luxembourg. All Rights Reserved.

La société luxembourgeoise Skype, spécialisée dans les logiciels de téléphonie par IP, est entrée en phase de test concernant un service payant de messagerie vocale. Sa mise sur le marché est prévue pour le printemps 2005. Cette messagerie vocale sera intégrée à la gamme de services payants de l'éditeur. Le logiciel Skype est actuellement gratuit et permet de joindre n'importe quel internaute de par le monde par une technologie dérivée du peer-to-peer. Les communications sont totalement gratuites, mais face à la concurrence des opérateurs téléphoniques classiques, la société a décidé de proposer des services payants à ses utilisateurs.

L'ADSL À 2,30 DOLLARS PAR MOIS EN INDE !

En Inde, un consortium dirigé par la société Aksh Broadband Limited (ABL) s'efforce de concrétiser un projet d'équipement du pays en haut débit. D'ici 2007, chaque Indien devrait avoir accès à Internet à un débit d'au moins 2 Megabits par seconde, à partir de la somme très modique de 2,30 dollars par mois. Cet environnement favorable à la baisse des tarifs du haut débit pourrait faire des émules dans d'autres pays... Un exemple pour la France et ses nombreux FAI ?



Un revirement de situation pour le moins incongru.



LA FNAC VA PERMETTRE DE HACKER LES DRM !

Le directeur général de Fnacmusic, François Montboisse, a annoncé officiellement la sortie d'un logiciel capable de craquer les DRM (Digital Rights Management) du propre site de la Fnac, Fnac music, pour rendre compatibles les fichiers proposés à la vente sur ce portail avec les baladeurs MP3. Moins de 20% des baladeurs MP3 distribués à la FNAC pendant la période de Noël étaient compatibles avec son service de musique en ligne. Le logiciel, légal, pourrait pourtant bien vite rendre la Fnac hors-la-loi si la "loi Eucd" sur les droits d'auteurs numériques était appliquée au logiciel.

PÉKIN RASE LA RUE DE LA SOIE, FLEURON DE LA CONTREFAÇON

La rue de la Soie, fleuron du commerce de contrefaçons aussi célèbres auprès des touristes chinois qu'étrangers, a subi un triste sort. Les stands et boutiques de la fameuse rue pékinoise de trois mètres de large sur plusieurs centaines de mètres de long, ont été rasés au Bulldozer. Raison invoquée : des problèmes de sécurité en cas d'incendie... Mais officieusement, c'est à l'Ambassade américaine que l'on doit ce carnage. Le bâtiment se trouve justement au bout de la rue de la Soie... L'ambassade a d'ailleurs félicité la municipalité pour cette action répressive. Rien n'est un hasard avec les USA : la démolition a eu lieu quelques jours seulement avant l'arrivée en Chine de Don Evans, le secrétaire américain au Commerce : ce dernier avait fulminé contre le non-respect de la propriété intellectuelle, durant une conférence de presse à Pékin en 2003, en prenant pour exemple un DVD pirate du film Kill Bill qu'il avait acheté à 1 € sur cette même rue... Quand l'Amérique demande, la Chine exécute ?



L'ADSL 2+ DE FREE : RECORD DE DÉBIT !

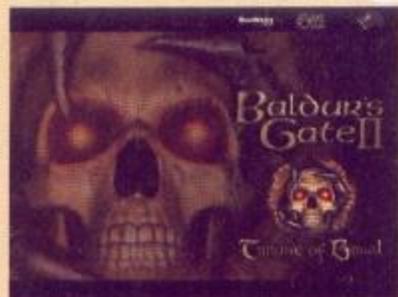


Les clients hallucinés de la nouvelle offre ADSL 2+ du FAI Free ont profité de l'augmentation de leur débit... qui vient de passer à 20 Mb/s ! Jusqu'alors, le record de Free était de 15 Mb/s théoriques. Voici la deuxième bonne nouvelle : l'offre est proposée sans changement de prix ! 29,99 euros par mois TTC sans autres frais pour un débit inégalé par les autres FAI, sauf par le câble qui propose un débit identique, mais pour la somme de 59,90 euros... Cette formule est toutefois réservée aux nouveaux clients Free dégroupés et équipés de la FreeBox v4. La couverture de l'ADSL 2+ ne concerne pas encore tout le territoire français, cependant. Free se place désormais en tête des FAI les plus rapides en devançant l'opérateur historique France Télécom qui lui propose "seulement" du 18 Mb/s également en ADSL 2+, sur Paris uniquement.

>> BYE BYE TITUS

INTERACTIVE

En redressement depuis le mois de juin 2004, l'éditeur de jeux vidéo Titus Interactive a vu prononcée à son encontre une liquidation judiciaire début janvier. Le groupe, qui possède plusieurs filiales à l'international, était dans une situation qualifiée de désespérée par le Tribunal de commerce qui, après avoir prolongé la période d'observation de l'éditeur, a finalement pris cette décision radicale. Précisons que la dette du groupe était à hauteur de 33 millions



d'euros. Toutefois, certaines filiales britanniques, américaines et japonaises ont échappé à la sentence. Titus était principalement connu pour son jeu Baldur's Gate. Depuis l'année 2002, le marché du jeu vidéo français est en crise : rappelons nous, cette

même année, la liquidation des deux éditeurs Cryo Networks et Calysto.

>> LA TV PAR SATELLITE SUR MOBILES EN CORÉE



La Corée du Sud vient de lancer, mi janvier en exclusivité mondiale, la première diffusion de chaînes de télévision satellitaires... sur téléphones portables ! En cours



LE SITE WEB

CHINOIS

DE NIKE PIRATÉ!



Le site Internet chinois de Nike, le géant de l'industrie du sport, a été hacké ! La prouesse a été réalisée par un certain " Danny " : ce dernier a tenu à afficher sur la page d'accueil du site ses meilleurs vœux pour la nouvelle année 2005 ! Avec une rapidité fulgurante, dans la nuit du 31 décembre au 1er janvier, Danny a remplacé la page d'accueil du portail chinois par son message " Hacked by Danny, Happy New Year", le tout en lettres rouges sur fond noir. Le message est resté affiché quelques dizaines de minutes tout de même ! La firme a réussi à rétablir rapidement son site Web dans la nuit du 31. Ce dernier est basé sur une plate-forme Microsoft IIS/5.0.

BILL GATES VA BREVETER LE "CTRL + ALT + SUPPR"!

Esérons que Bill Gates aime le bleu : lors d'une représentation au CES de Las Vegas, Mr Bill a assisté impuissant à l'apparition d'un écran bleu, la panne informatique ultime nécessitant de rebooter votre machine ! Il était en train d'exposer le " keynotes " de Microsoft concernant l'électronique grand public...

Deux magnifiques plantages de son système se sont produits, un lors de la présentation de Microsoft Media Center et l'autre durant une démonstration sur console Xbox. Heureusement que M. Gates est entouré de Conan O'Brien, co-animateur du keynotes, à l'humour décapant : celui-ci a lâché un " Déjà neuf personnes licenciées " provoquant l'hilarité de l'assistance. Les employés, eux, ont dû rire un peu jaune...



EXEEM, QUAND SUPRNOVA.ORG

FAIT DES ÉMULES...

Le site Suprnova.org, qui avait été mis à mal il y a peu, ne pouvait plus diffuser de liens .torrent. Qu'à cela ne tienne ! Le site travaillerait en ce moment à une nouvelle version du client et du protocole BitTorrent. Le projet, qui répondrait au nom d' " eXeem ", proposerait une décentralisation du réseau : chaque client va devenir un tracker ou un serveur potentiel, à l'instar d'autres réseaux de P2P tels qu'Overnet, notamment. Le site compte ainsi lutter contre le piratage sur le réseau en rendant difficile la suppression des tables des sources correspondant aux fichiers disponibles en téléchargement.



CHARITY BUSINESS

Le groupe MasterCard International a lancé un avertissement aux usagers des cartes de

crédit éponymes de la firme concernant les dons destinés à aider les victimes du raz-de-marée d'Asie du Sud. En effet, des fraudeurs auraient créé de faux sites Internet appelant aux dons. Ces derniers, utilisant la technique dite de " phishing ", créent un site quasi identique à celui d'une banque le plus souvent, sur lequel on demande à l'internaute toute une série d'informations personnelles. MasterCard International rappelle à ses clients de ne passer que par des sites officiels d'agences humanitaires pour effectuer leurs dons en toute sécurité.



d'implantation et toujours à l'essai, la commercialisation du service est prévue fin mai 2005. Les programmes seront proposés en haute définition, le tout rendu possible par la technologie Toshiba. L'opérateur TU Media proposera à ses clients 14 chaînes vidéo et 24 audio ! Côté équipement, c'est Samsung Electronics qui le premier a présenté un modèle de téléphone compatible avec la technologie nécessaire à la réception des chaînes sur écran 2,2 pouces. L'autonomie de l'appareil sera de deux heures, fonctionnant sur piles, pour la somme modique de... 800 dollars américains environ. Le marché est porteur : 76% de la population du pays est équipée de portables.

SKULL.D, UN VÉR TROJAN SUR MOBILES

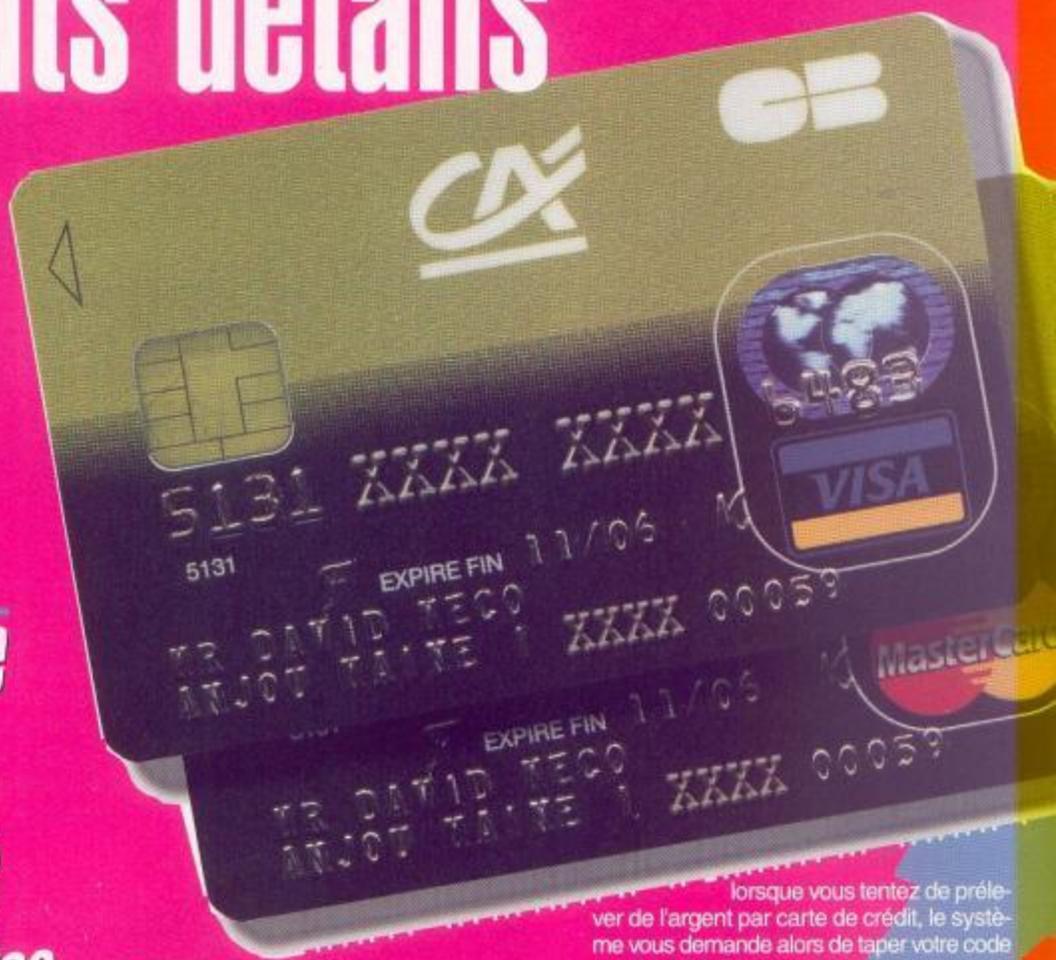
Une nouvelle version du cheval de Troie Skulls est apparue sur les réseaux de téléphonie mobile. Son nom : Skulls.D. Le ver-cheval de Troie se manifeste en affichant une tête de mort en plein écran sur le mobile en question. Cette version prend la forme d'un lecteur de fichiers Macromedia Flash et concerne uniquement les appareils fonctionnant sous le système d'exploitation Symbian Series 60. Passer des communications est toujours possible, mais l'accès à tous les autres menus et fonctions, dont l'installation d'applications, est bloqué. Si vous êtes infecté, il est alors nécessaire de réinitialiser votre portable, sans possibilité de sauvegarde de vos données. Skulls.D se propage par le biais de forums proposant des programmes à l'origine inconnue. Restons attentifs !



CARTES DE CRÉDIT

et petits détails

*Mécanismes
et situations
à connaître
pour tout
savoir sur le
fonctionne-
ment de ces
petites cartes
en plastique
et éviter tout
problème !*



Vous êtes-vous jamais demandé pourquoi le Guichet automatique fonctionnait en tapant son code secret (le code PIN, Personal Identification Number) tandis qu'une simple

signature suffit lorsque vous faites vos achats par carte de crédit? La réponse est que seule la société qui a émis la carte de crédit est à même d'effectuer un contrôle efficace du code PIN. Les commerçants peuvent uniquement effectuer des contrôles partiels. C'est la raison pour laquelle le code PIN n'a jamais été nécessaire à l'utilisation des cartes de crédit. Même si ce système serait sans doute utile... En effet,

lorsque vous tentez de prélever de l'argent par carte de crédit, le système vous demande alors de taper votre code confidentiel. Même si tout le monde n'est pas forcément au courant, il faut savoir que les cartes de crédit possèdent elles aussi un code PIN.

Autre question: lorsque vous réservez une chambre d'hôtel et qu'on vous demande votre carte de crédit, pourquoi le jour même peut-il y avoir certains problèmes avec le plafond de crédit, tandis que tout redevient normal dès le deuxième jour ?

Faire une réservation et rester "sans argent"

Nombreux sont ceux qui ont connu cette situation, notamment en vacances,



American Express est la carte idéale de Big Brother

et plus particulièrement aux Etats-Unis. On réserve un bel hôtel pour quelques jours et on observe une situation analogue à celle qui vient d'être décrite. En voici la raison: comme vous le savez déjà, une carte de crédit ordinaire est plafonnée au niveau des dépenses. Une autorisation de dépense génère habituellement un hold, une sorte de préemption, sur la somme en question.

AMERICAN EXPRESS VOUS OBSERVE

Les cartes de crédit sont généralement plafonnées, mais la carte American Express (AMEX) fonctionne autrement. AMEX est la carte idéale de Big Brother (celui d'Orwell, pas celui d'Aran Endemol): elle accepte les transactions en fonction des utilisations passées, de l'historique des paiements et des informations financières du propriétaire de la carte. De plus, par convention, avec la carte American Express, aucune machine ne dira jamais "non" à un client. Si le système d'autorisation électronique estime que la transaction est risquée, il demandera alors au commerçant de se mettre directement en contact avec la société émettrice qui voudra peut-être également parler avec le propriétaire de la carte. Ce dernier se verra demander certaines informations - jamais deux fois les mêmes - à caractère personnel voire financier. Ceux qui tiennent au respect de leur vie privée feraient bien d'y réfléchir à deux fois avant de demander une carte American Express.

AMERICAN EXPRESS

En pratique, le hold bloque ce montant (même s'il n'y a aucun débit, l'argent reste sur votre compte). Dès que vous réservez un hôtel pour une semaine, le montant équivalent à la réservation est bloqué, (un montant qui peut parfois être élevé). Mais lorsque vous allez ensuite manger une pizza, une addition même peu salée peut alors poser quelques problèmes.

Le jour suivant, en revanche, la première nuit a effectivement été débitée de votre carte; un montant bien moins élevé que la totalité de la somme qui, en attendant, a été libérée et de nouveau mise à votre disposition.

Chez les commerçants en revanche, la procédure n'est pas la même. Lorsque vous faites un très gros achat, en demandant l'autorisation, le commerçant pourrait se voir répondre par la société émettrice qu'un contrôle supplémentaire est nécessaire. Dans certains cas, cela peut même passer par un coup de téléphone. Lorsque prévaut le bon sens (ou l'engineering social !), le plafond peut être limité à la seule transaction.

Un plafond jamais suffisant

Certaines personnes prennent spécialement une carte de crédit lorsqu'elles partent en vacances. Elles partent et s'aperçoivent bien vite que les dépenses autorisées par cette carte sont plafonnées et que ce plafond est très vite atteint. Votre compte est bel et bien approvisionné, mais impossible de dépenser l'argent placé dessus ! Solution : téléphoner à la société émettrice et lui demander d'augmenter le plafond.

Par expérience, la personne à l'autre bout du fil fera tout pour vous en empêcher. Elle vous dira qu'il faut envoyer un fax plutôt qu'un courrier recommandé, que cela nécessitera une quinzaine de jours, qu'il faudra une autorisation de votre banque et je ne sais quoi encore. Tout est faux. Ils ont la possibilité de le faire et ce, immédiatement, sans recevoir de fax. Pour se voir

POUR UNE CARTE DE CRÉDIT SÉCURISÉE

- 1) signez-la dès réception et ne la laissez pas en blanc (il est vrai qu'on vous demande une pièce d'identité lorsqu'elle n'est pas signée, mais si on vous la vole, n'importe qui pourra alors la signer et l'utiliser en toute liberté);
- 2) portez votre carte ailleurs que dans votre portefeuille;
- 3) gardez une trace des données de votre carte en lieu sûr, et à un emplacement différent de celui où vous rangez votre carte;
- 4) Ne quittez pas votre carte des yeux pendant une transaction et récupérez-la dès que possible;
- 5) Conservez les tickets en lieu sûr ou détruisez-les. Ne les jetez jamais!
- 6) Contrôlez vos relevés de compte et comparez-les aux tickets ou autres notes de frais;
- 7) Prévenez à l'avance la société émettrice de tout changement de domicile;
- 8) Ne prêtez jamais votre carte, à quiconque;
- 9) Ne signez jamais un reçu en blanc. Barrez tous les espaces vides sur le reçu;
- 10) Ne communiquez pas les données de votre carte aux personnes dont vous n'êtes pas sûres.



accorder une hausse du plafond, il vous faudra insister, poliment mais fermement. Il y a ceux qui s'inventent des situations d'urgence (nous sommes à l'étranger, notre voiture est tombée en panne, nous devons en louer une autre, il y a eu un accident etc.). Il y a aussi ceux qui téléphonent de chez eux, en racontant qu'ils sont à l'étranger et ont besoin d'argent!

crack

CHAOS au casino!



Que faire lorsqu'une bande de pirates sortis de nulle part, prend en otage votre site? C'est arrivé à certains mais tous ne s'en sont pas sortis indemnes...

Bon nombre d'entre eux courent toujours!

D'autres en revanche ont eu beaucoup moins de chance, comme Multibet (<http://www.multibet.com>), une société de paris dirigée par l'australien Terry Lillis, exerçant ses activités dans une dizaine de pays.

Les maître-chanteurs se manifestent et réclament à Lille plus de 15 000 euros en échange de leur protection. Il les envoie balader. Cinq minutes plus tard, ils bloquent son site par une attaque DDoS : un coup de massue qui met un terme à son business pendant



▲ *Après les attaques menées contre les casinos online, les joueurs ne sont plus les seuls à être dépouillés!*

Arrêtée en juillet dernier, une bande russe mettait hors d'usage les serveurs des agences anglaises spécialisées dans les paris, en lançant des attaques DDoS, et en demandant ensuite une contrepartie financière pour cesser ses activités frauduleuses. La National Hi-Tech Crime Unit britannique a collaboré avec les autorités russes jusqu'à ce que les trois coupables soient retrouvés. Agés de 21 à 24 ans, ils réclamaient des sommes allant de 10 à 20 000 dollars, avec des pointes à 55 000. Mais il a fallu du temps pour les débusquer. Depuis octobre 2003 date à laquelle les plaintes ont été déposées, les pirates sont parvenus à leurs fins pour un montant de plusieurs centaines de milliers d'euros, si ce n'est plus. A la fin, on a même découvert qu'ils avaient cherché à faire chanter les parieurs américains à l'approche du Super Bowl, la finale des finales du football américain.

QU'EST-CE QU'UN DDoS?

DDoS signifie Distributed Denial of Service. Attaque par laquelle une multitude de systèmes compromis (c'est pour cela qu'il s'appelle "réparti") bombarde malgré elle une cible, qui croûte sous un nombre de paquets trop importants pour ses capacités et ne peut plus effectuer ses fonctions.

providers telematiques, dont les services
peuvent être rendus inaccessibles suite
d'importantes attaques DDoS s'ils ne paient
pas la " rançon " exigée.





HACKER
Magazine

Tout ce que les autres n'ont pas osé vous dire !