

# HACKER NEWS MAGAZINE

12<sup>F</sup>

**Piratage, Intrusion,  
Sécurité, Internet,  
Espionnage, Filtrage,  
Mots de passe, Virus...**

**News:** toute l'actualité underground - **GNUTELLA:** Interview exclusive -  
**Scour:** le cousin de Napster - **DVD:** le dézonage expliqué - **Defcon:** le  
rendez vous des pirates - **Techno:** les magnétoscopes numériques -  
**Microsoft:** chronique d'un bogue annoncé - **Yahoo!** Internet en danger ?  
**Windows:** les mots de passe secrets



M 5528 - 1 H - 12,00 F - RD



Trimestriel - 12 FF - DOM 15F - 85 FB - 3.5 FS - 84 FL - 20 DH - 1400 CFA - \$2.95

# EDITO HACKER MAGAZINE

**A**u travers de ces 32 pages, il ne s'agissait pas pour nous de vous apporter une information aseptisée mais bien un rédactionnel alternatif où la ligne éditoriale sera totalement indépendante.

Un choix que nous entendons maintenir avec le soutien du groupe qui nous édite (Hagal Aria) qui en a fait un principe directeur avec d'autres magazines tels que l'Officiel du Net ou PCNews.

Des news du milieu "underground", des dossiers revenant sur des points d'intérêt majeurs (piratage, virus, cryptage, etc.) et des interviews pour compléter le tout, voilà en résumé le contenu de Hacker News Magazine. Comme vous pourrez le constater, nous ne vous vendons pas des pages vides, ni de la démagogie de seconde zone. Il s'agit plus d'informations en rapport avec des thèmes peu ou mal traités dans la presse grand public. Notre objectif n'est certainement pas de vous inciter à pirater mais de vous informer au mieux sur ce milieu encore nébuleux pour la plupart d'entre vous. Nous espérons que ce premier numéro, encore imparfait, vous séduira...

*Eric Le Fauconnier*

## Taiwan s'entraîne à la guerre électronique

Après la Chine l'année dernière, c'est au tour de Taïwan, son ennemi de toujours, de simuler une guerre informatique. Cette dernière aurait mis au point pas moins de 2000 virus à utiliser en cas de conflit électronique. Les prémices de cette défense électronique avaient vu le jour, l'année dernière avec les premiers tests grandeur nature pour valider la capacité de protection. Cette année la priorité a été donnée sur les possibilités offensives du dispositif.  
Source: LibertyTimes & AFP

## Cryptographie:

### Modification de la loi le 30 septembre !

On connaissait la réticence de la France dans le domaine de l'encryptage des données, qui avait pourtant légèrement assoupli sa position sous la pression internationale (la France faisait partie des états les plus restrictifs avec la Chine!) avec un décret en 1999. C'est cette fois l'Europe qui fait un pas décisif en autorisant les ventes de logiciels d'encryption au sein de la communauté européenne sans aucune autorisation préalable. Quelques exceptions subsistent mais c'est un premier pas vers la libéralisation. Dans l'immédiat, le décret français de 1999 prévaut sur la directive européenne.



Linux n'est pas le seul système basé sur Unix, il existe aussi FreeBSD

## Smurfing, voilà peut être comment des adolescents ont fait tomber Amazon, Yahoo! ...

Internet est constitué d'un ensemble de réseaux interconnectés entre eux; certains d'entre eux, pour ne pas dire un grand nombre, permettent ce que l'on appelle la connexion directe via adresse IP. Celle ci permettant d'envoyer des requêtes à un réseau qui les livre à toutes les machines connectées à celui ci, ayant ainsi un effet multiplicateur. Si la requête demande une adresse en réponse comme par exemple la commande "ping" qui teste la réactivité d'un serveur, il suffit alors de donner une adresse de retour volontairement erronée comme par exemple celle de yahoo! pour que celui ci soit rapidement submergé de réponses qui auront tôt fait de faire exploser le trafic et donc de faire tomber le serveur. Cette technique, appelée le "smurfing" du nom du premier programme autorisant ce genre d'attaques "Smurf". Un jeu d'enfant qui pourrait être évité si les réseaux étaient mieux configurés pour éviter ce genre de requête IP.

## Faites vous assurer !

Le marché de l'assurance dans le domaine de la sécurité informatique est en passe d'exploser selon le magazine Fortune. Les assureurs multiplient d'ailleurs les offres qui vont de 5000€ jusqu'à parfois plus de 100 000€. L'IS (Insurance Information Institute) considère que ce secteur représentera plus de 2,5 milliards d'euros d'ici à 5 ans.

Hacker News Magazine  
177, rue des Martyrs  
76150 Maromme  
France  
Tél.: 02.32.82.30.87

Directeur de la publication:  
Marc Segault

Rédacteur en Chef:  
Grégory Peron

Imprimerie: OGI

Commission paritaire: en cours

Dépôt légal: à parution

RCS PARIS B421097973  
SARL au capital de 85000 FF

Tous droits réservés

Hacker News Magazine est une  
publication du groupe Hagal Aria

## Yahoo! Internet Life ? Plutôt death que life !

Le magazine Internet, Yahoo! Internet Life vient de cesser sa parution officiellement pour un problème entre le groupe de presse VNU, qui exploitait le nom, et la maison mère de

Yahoo! aux Etats Unis. D'après des sources bien avisées, il conviendrait d'ajouter à cela des ventes extrêmement décevantes bien inférieures à ce qui était prévu à l'origine...

### SMS Flooder: attaque virale sur cellulaire

Un pirate informatique du nom de "HSE" aurait écrit un programme en visual basic 5.0 qui utiliserait le réseau téléphonique pour transmettre de grandes quantités de messages SMS. Il permettrait notamment de submerger un utilisateur en faisant sonner son téléphone sans arrêt et de saturer sa mémoire. Le phénomène semble limité à la seule Allemagne dans l'immédiat mais "SMS flooder" pourrait bien évoluer et s'adapter aux autres réseaux téléphoniques. A suivre...

### La confiance règne

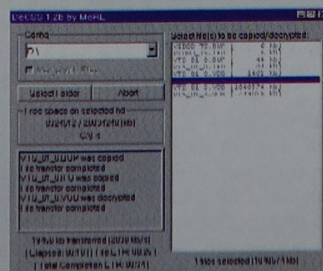
Alors que la banque suisse UBS et la Barclays connaissent de petits soucis avec les pirates informatiques, un récent sondage effectué à Londres montre que 47% des interviewés ont moins confiance dans la banque en ligne que dans la banque traditionnelle. Seulement 31% pensent que leur argent et leurs données personnelles sont en sécurité. Espérons que le financier Bernard Arnault avec son projet de banque en ligne ; Zebank, saura un peu mieux convaincre les français. <http://www.zebank.com>

## Piratage des DVDs, 1-0 pour Hollywood

Il y a quelques mois, un jeune Norvégien développait DeCSS, un logiciel permettant de lire des DVDs sous Linux. Rapidement adapté pour Windows, le logiciel est immédiatement proposé en téléchargement sur un certain nombre de sites Web dont celui de notre confrère, le magazine 2600. L'industrie cinématographique voyant ses intérêts menacés réagit peu après en portant plainte contre Eric Corley, l'éditeur de 2600 via la très puissante MPAA (Motion Picture Association of America). Le juge Lewis Kaplan en charge de l'affaire a donc décidé, le 17 août dernier, de faire suspendre

le téléchargement de DeCSS. Celui ci permettant en plus de la simple lecture de DVDs, de faire sauter la protection anti piratage de ces derniers.

<http://www.2600.com>



Très léger, DeCSS fonctionne parfaitement !

## Explosion de la criminalité informatique

C'est ce qui ressort de la dernière édition du rapport du Computer Security Institute (CSI) réalisé avec le FBI. Nous vous proposons ci après quelques chiffres extraits de ce document:

**90%** des interviewés avouent avoir détecté des failles de sécurité dans leur système informatique au cours des 12 derniers mois.

**74%** concèdent avoir eu un préjudice financier lié à ces failles.

**42%** sont capables de quantifier ce préjudice qui s'élève pour 273 sociétés à plus de 265 589 940 euros (A noter que la moyenne sur les 3 dernières années était de 120 240 180 euros.)

Dans 8 des 12 catégories, les pertes financières n'ont jamais été aussi importantes auparavant. Pour 4 catégories le cumul des 3 précédentes années n'atteint même pas les pertes de cette année.

La conclusion semble couler de source; la criminalité informatique sera l'un des défis majeurs du 21e siècle.

"Les résultats de ce rapport nous fournissent des données particulièrement intéressantes. Ces informations seront non seulement communiquées aux Congrès pour souligner les besoins en terme de moyens au niveau national mais aussi pour identifier les futures tendances criminelles afin d'être le plus pro actif possible. Cela nous permettra d'affecter rapidement des ressources afin que ces "tendances" ne se transforment pas en crises."

Bruce J. Gebhardt bureau de Californie du FBI

A voir: [http://www.gocsi.com/prelea\\_000321.htm](http://www.gocsi.com/prelea_000321.htm)

## Un top model de Palm !

Un rapprochement pour le moins surprenant entre le constructeur d'assistants personnels, Palm avec le mannequin Claudia Schiffer. Le but étant de lancer un Palm Vx aux couleurs du célèbre Top Model allemand, qui officiellement s'est occupé de choisir elle-même les logiciels livrés. Pas de grands changements pour le produit, mais plutôt une modification d'ordre esthétique (couleur du boîtier bleu métallisé.) Cet assistant personnel est vendu depuis septembre, mais uniquement en ligne sur le site officiel de Claudia Schiffer.



<http://www.claudiaschiffer.com> - <http://www.palm.com>

## en bref l'actualité underground

### Ils sont fous ces 'Ricains !

Un neurologue américain, Christopher Newman, atteint d'une tumeur maligne au cerveau vient de déposer plainte contre neuf sociétés de télécommunications dont Motorola. Il considère que c'est l'usage du téléphone portable qui en est la cause. A ce titre il demande plus de 800 millions d'euros de dédommagements.

Source: Reuters

### L'histoire du policier qui aimait bien les petites filles...

Philip Amatulli, policier à New York, aime beaucoup, mais alors beaucoup les petites filles, surtout lorsqu'elles sont mineures. Il vient de se faire appréhender pour avoir, via Internet, proposé à ce qu'il croyait être une mineure d'avoir des relations sexuelles avec lui. En fait c'était un agent des douanes... il risque jusqu'à 15 ans de prison et 250 000 euros d'amende. Il ne plaisante pas avec les pédophiles l'Oncle Sam (et c'est tant mieux !)

Source: Reuters

### Internet: Bientôt une heure universelle ?

Le Premier ministre britannique Tony Blair souhaitait faire de Greenwich, déjà référence du temps universel, celle de l'Internet. Cette initiative aurait échoué suite à des difficultés techniques, du fait des incompatibilités avec Internet Explorer, le navigateur Web de Microsoft.

Source: The Independent

### Hackers: gentils ou méchants ?

"Je vous invite à rejoindre le gouvernement ou le secteur privé [...], à vous ranger du côté de la défense", a déclaré Art Money, vice-secrétaire d'Etat à la Défense, pendant le premier jour du Defcon, le plus grand rassemblement mondial de pirates informatiques (Las Vegas.)

### Vos résultats à l'avance !

Quatre heures avant la parution officielle des résultats d'entrée à l'université chypriote, ceux-ci ont été donnés à la radio locale. Le ministère de l'éducation

souçonnerait un piratage du site Web où devaient être publiés les résultats. A quand la modification des résultats ?

### Dans le genre réac !

Dow Chemical a annoncé fin juillet, le licenciement d'une cinquantaine de salariés et la mise à pied de plus de 200 autres pour quatre semaines. La raison de ces mesures radicales ? Avoir conservé, envoyé ou retransmis des emails à caractère violent ou pornographique... Un bon conseil: si vous recevez la photo d'une jolie fille en maillot de bain au travail, effacez vite ce courrier électronique car si vous travaillez dans une filiale de Dow Chemical (39 000 personnes dans le monde) vous pourriez bien avoir des problèmes !

[www.dow.com](http://www.dow.com)

### Saddam, grand démocrate !

L'Irak vient d'ouvrir un espace où la population pourra accéder librement à Internet. Le ministre en charge a affirmé par ailleurs que les Nations Unies avaient refusé de donner leur accord à certains contrats dans le domaine des télécommunications, ce qui aurait retardé l'ouverture de ces centres. Info ou intox ?

Source: reuters

### Gratuit... enfin presque gratuit

Bill Quinn n'est pas prêt d'oublier son abonnement gratuit souscrit auprès de Comuserve (Etats Unis). Il a en effet été débité de plus de 21000 F au bout d'un mois d'utilisation alors qu'il avait installé un kit de connexion gratuit ! Après enquête, la filiale d'AOL a tout de même décidé de lui rembourser 11 000 F après s'être aperçue que son compte avait été piraté par des hackers anglais, pays où l'utilisation de Comuserve est payante.

### Il n'en fallait pas moins !

Dans un cas classique, il aurait suffi d'un pasteur pour se confesser, il en aura fallu pas moins de 4500 pour Bill Clinton. C'est en effet à Chicago début août, lors de la "réunion des pasteurs", que celui-ci a décidé "d'ouvrir son cœur".

# NAPSTER, GNUTELLA & SWAPOO

On connaissait déjà Napster, Gnutella ou Scour (voir page 27) qui permettait l'échange de fichiers MP3 ou vidéos. Voici venu Swapoo sur le marché des logiciels d'échange de fichiers. A l'origine prévu pour permettre aux internautes de s'échanger des logiciels gratuits (freewares), Swapoo s'est vite trouvé une spécificité : l'échange de jeux pour consoles plus ou moins récents. Le fonctionnement du logiciel se situe entre Napster (gestion des

fichiers disponibles chez les utilisateurs) et Gnutella (gestion des connexions des utilisateurs aux serveurs), Swapoo se contente de gérer les connectés ainsi que leurs demandes de téléchargement entre eux. De plus, le logiciel permettra à terme d'intégrer une liste de fichiers interdits, de quoi, en théorie, empêcher le piratage. A suivre.

[www.swapoo.com](http://www.swapoo.com)

Source: Yahoo!

## A défaut d'avoir un système sans bogues...

"S'il y a jamais eu une industrie où aucune compagnie n'a été leader pendant deux générations de suite, c'est bien celle des jeux vidéo. [...] La puissance contenue dans notre console (ndlr: la Xbox) la conduit vers un tout autre niveau... Vous ne penserez même pas que la Playstation 2 et la Xbox appartiennent à la même génération."

Voilà les quelques lignes qui résument l'interview donnée au magazine américain The Red Herring par Bill Gates lorsqu'il a été interrogé sur la console de jeux que prépare Microsoft, la Xbox. Celle-ci devrait sortir l'année prochaine.

Microsoft  
**Office**

Bill Gates dans The Red Herring

# news, rumeurs, news, exclusif, news, brèves —>>> les Actualités

## Mais que fait Greenpeace ?

Pendant que les écolos de Greenpeace ennuiant les autorités françaises à propos du nucléaire, les Américains renforcent quant à eux, en toute quiétude, leurs dispositifs de sécurité. Ainsi la toute nouvelle agence chargée de la sécurité en matière de nucléaire, la NNSA (National Nuclear Security Administration), a vu la nomination de John Gordon à sa tête ; celui-ci a d'ores et déjà annoncé un durcissement de la politique en matière de protection informatique. Conséquences probables de la disparition temporaire mais

remarquée, en juin dernier de deux disques durs contenant des données ultra sensibles de la base militaire nucléaire de Los Alamos. Dans le cadre de son enquête, le FBI a utilisé des détecteurs de mensonges (polygraphes) pour déterminer les responsables de cette mystérieuse disparition ; Les résultats de l'enquête ne sont pas encore publics à l'heure où nous écrivons ces lignes. Il semblerait donc que pour les Américains les enjeux du nucléaire soient tels qu'ils renforcent les services de contre espionnage.

## Du rififi chez les Japonais

Un site américain spécialisé dans l'information relative au monde du renseignement a publié début juillet, une liste de plusieurs centaines de noms de personnes travaillant pour le PSIA (Public Security Investigation Agency), les services secrets japonais. Adresses, numéros de téléphone, fonctions, tout est donné en pâture aux internautes qui peuvent ainsi voir qui travaille dans ces services plus si secrets que cela. On apprend également que sur les 1700 agents, 1100 travaillaient sur des affaires intérieures et 600 sur des affaires

d'espionnage à l'étranger. Quatre jours après la publication de cette liste, deux agents du FBI auraient appelé John Young, le webmaster du site, pour lui intimer de la retirer immédiatement. Celui-ci a refusé en précisant toutefois qu'il ne publierait pas les noms des deux agents du FBI également présent sur la liste puis se ravisa deux jours plus tard sous prétexte que le FBI l'aurait mis en garde contre les conséquences fâcheuses que pourrait avoir pour lui, le fait de les rendre publiques.



## Cybiko = Game Boy + Palm

Alors que les Anglais sont en passe de faire passer un nouveau projet de loi, la RIP (Regulation of Investigatory Powers), qui permettra au gouvernement de sa majesté d'effectuer des écoutes électroniques (courrier électronique, Web, etc.) au même titre que les écoutes téléphoniques.

Les Etats Unis viennent d'annoncer par la voix du directeur de cabinet de la Maison blanche, John Podesta, une proposition de loi équivalente par l'administration Clinton. Les premières ébauches de celle-ci, Carnivore, ont provoqué une véritable

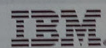


levée de boucliers tant de la part des professionnels que de l'opinion publique. Pourtant, c'est bien chez nos "amis" anglais que la situation est la plus préoccupante car contrairement aux Etats Unis, les services de renseignement britanniques n'auront besoin d'aucune autorisation de la part d'un juge pour mettre en place ces écoutes. Une situation tout à fait incroyable qui pourra permettre tous les excès sans aucune limitation.

Les entreprises anglaises peuvent déjà surveiller et espionner leurs salariés en toute impunité sur leur lieu de travail et ce, sans que la moindre autorisation ne soit nécessaire. Un état de fait déjà préoccupant qui, espérons-le, ne trouvera pas d'écho dans notre beau pays des droits de l'Homme et de la Liberté !

## IBM à l'heure Linux

Des chercheurs de la société IBM ont mis au point une montre de 5,6 cm sur 4,8 intégrant linux 2.2. Cette montre peut communiquer avec des PC ou des téléphones portables, elle permet en outre de lire des messages électroniques courts et inclut un calendrier, un carnet d'adresses et une liste de tâches à faire. L'objectif d'IBM était de démontrer la viabilité de linux sur des systèmes de petite taille.



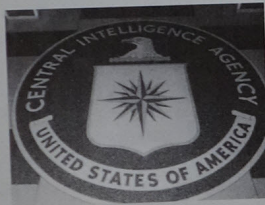
Tous les trois mois, retrouvez  
toute l'actualité alternative dans  
Hacker News Magazine

## en bref l'actualité underground

### Souriez, vous êtes surveillés

Vous vous croyez en sécurité chez vous lorsque vous êtes sur votre ordinateur avec la connexion Internet coupée ? Et bien c'est une erreur ! Les Américains ont mis au point une technologie, Tempest, permettant de capter les ondes électromagnétiques émises par un ordinateur. En d'autres termes, Tempest permet purement et simplement de visionner à distance les écrans d'ordinateurs sans avoir la moindre connexion physique avec celui-ci. Autant vous dire que cette technologie provoque toutes les convoitises; ainsi en début d'année, un israélien a t'il été condamné par un tribunal américain pour avoir voulu exporter sans autorisation préalable du matériel exploitant Tempest. Espérons que les libertés individuelles seront bien respectées, rien n'est moins sûr !

### En avant le gaspillage !



L'une des divisions des services secrets américains, le NFIP (Programme National de Renseignement E t r a n g e r ), auraient vu ses effectifs baisser de plus de 20%, soit 20 559 personnes, depuis le début de la déconfiture soviétique en 1991. Dans le même temps son budget a augmenté de 15% pour atteindre en 1999 5,4 milliards d'euros. Si les effectifs n'avaient pas été réduits, l'augmentation aurait été de près de 45% ! Sachant qu'il faut un franc par jour pour nourrir un enfant africain, le budget de ce seul service permettrait de sauver plus de 100 millions de personnes par an ! A méditer...

### Après Napster, DivX ?

Alors que le logiciel/service de partage de fichier MP3, Napster, vit probablement ses derniers jours sous sa forme actuelle, une nouvelle menace se profile pour les professionnels du DVD: DivX. Méthode d'encodage vidéo, il promet de devenir rapidement la nouvelle coqueluche des internautes.

### La carte à puce fait des émules

Le gouvernement de sa Majesté vient par l'intermédiaire du Home Office de préconiser la mise en place des cartes à puce d'ici à 2003. Cela fait suite à la suite de la publication du dernier rapport sur les infractions à la carte bancaire au Royaume Uni. Ceux-ci montrent une hausse préoccupante du nombre de fraudes de près de 50% entre 1998 et 1999. L'organisme équivalent au GIE carte bleue français, l'APACS (Association for Payment And Clearing Services) a dorénavant déjà apporté son soutien à l'initiative. L'actualité de ces derniers mois avec notamment l'affaire Humpich a toutefois mis en avant les limites de la carte à puce et les risques de piratage. Plus de sécurité pour les Anglais mais cela sera-t'il suffisant pour endiguer cette nouvelle forme de criminalité ?

Source: The Guardian

### Apache 2.0, l'alternative à Windows IIS

Le serveur Web gratuit devrait voir une nouvelle version, la 2.0, avant la fin de l'année. Celle-ci intégrera le multitâche (plusieurs tâches effectuées en même temps), une plus grande compatibilité avec d'autres protocoles comme le Wap, et enfin devrait pouvoir être porté sur beOS, Windows ou Mac. Contrôlant déjà plus de 60% du marché des serveurs, Apache promet de renforcer sa position probablement au détriment du produit de Microsoft, IIS.

## Vol d'ordinateur, bientôt un mauvais souvenir ?

En 1998, le vol d'ordinateur a coûté plus de six milliards de francs, une somme colossale qui suscite tous les appétits. CyberTrak Systems Inc aurait peut-être trouvé la solution pour remédier à ce problème avec une technologie baptisée SecurePC. Actuellement en beta test au MIT (Institut de Technologie du Massachusetts), il serait presque indétectable et quasiment impossible à désinstaller. Le plus intéressant restant son mode de fonctionnement: Si un ordinateur avec SecurePC est volé et que la personne l'ayant récupérée se connecte à Internet, SecurePC alerte le poste de police le plus proche du point de connexion directement en leur envoyant un fax. Simultanément, les données et fichiers du propriétaire original sont rapatriés via le réseau et placés sur un serveur dédié. Double avantage donc, avec l'identification et l'arrestation des voleurs mais aussi une chance de récupérer les informations contenues sur l'ordinateur volé. [www.cybertraksystems.com](http://www.cybertraksystems.com)

### Cyber Jihad sur Internet

Un groupe de francs de pertes aux sites israéliens. En réaction, Israël a décidé de former une unité spéciale de lutte contre les pirates. Groups...



il y a quand même des fainéants !

# news, rumeurs, news, exclusif, news, brèves —>>> les Actualités

## Changez de look

"Quiconque disposant d'un ordinateur et d'une carte de crédit peut obtenir, presque instantanément, une carte de Sécurité sociale apparemment authentique, portant le nom et le numéro de son choix" écrit, James Huse, inspecteur général de la Sécurité sociale.

Cette phrase résume à elle toute seule la facilité pour se procurer de faux papiers sur le Net. Une simple recherche sur "fake id" ("fausse identité") et ce sont des centaines de sites qui sont immédiatement accessibles. Permis de conduire, diplômes, carte d'identité ou carte d'étudiant, il ne vous reste qu'à faire votre choix. Parmi les sites



repérés, photoïdcards et ses cartes de chasseurs de primes, fake-id et ses cartes d'identité américaines et Belvine qui propose presque tout ! L'ensemble de ces documents est souvent de très bonne qualité et à bas prix. Source: AFP

## Marre des Start Up !

Les habitants de San Francisco commencent à en avoir ras le bol des Start Up ou autres sociétés de la nouvelle économie. Un phénomène de saturation qui s'est concrétisé par une pétition qui a regroupé plus de 30 000 signatures pour exiger la limitation du nombre d'entreprises de ce type dans la ville. Cette réaction quelque peu radicale, résulte du fait que les start up occupent de plus en plus de locaux dans les zones industrielles ou des quartiers de banlieue à loyer modéré, zones traditionnellement réservées aux familles à revenus modestes ou aux artistes. Ceux-ci ne pouvant bientôt plus rester du fait de la hausse des loyers. La proposition de limitation vient, suite à un référendum, d'être repoussée de justesse.



Espérons que la Silicon Sentier de Paris ne posera pas les mêmes problèmes aux fabricants de tissus.

## A quand la prochaine attaque ?

L'association ISS (Internet Security Systems) a déclaré que de nombreux serveurs étaient actuellement affectés par des logiciels "zombies", qui pourraient permettre à des pirates informatiques de prendre leur

contrôle pour ensuite lancer des attaques de type DoS (Denial of Service). De nombreux sites marchands pourraient bien subir ce genre d'attaques au moment de Noël, une inquiétude prise très au sérieux par le FBI.

## Anglais, Américains même combat !

Alors que les Anglais sont en passe de faire passer un nouveau projet de loi, la RIP (Regulation of Investigatory Powers), qui permettra au gouvernement de sa majesté d'effectuer des écoutes électroniques (courrier électronique, Web, etc.) au même titre que les écoutes téléphoniques. Les Etats Unis viennent d'annoncer par la voix du directeur de cabinet de la Maison blanche, John Podesta, une proposition de loi équivalente par l'administration Clinton. Les premières ébauches de celle-ci, Carnivore, ont provoqué une véritable levée de boucliers tant de la part des professionnels que de l'opinion publique. Pourtant, c'est bien chez nos "amis" anglais que la situation est la plus préoccupante car contrairement aux Etats Unis, les services de renseignement britanniques n'auront besoin d'aucune autorisation de la part d'un juge pour mettre en place ces écoutes. Une situation tout à fait incroyable qui pourra permettre tous les excès sans aucune limitation. Les entreprises anglaises peuvent déjà surveiller et espionner leurs salariés en toute impunité sur leur lieu de travail et ce, sans que la moindre autorisation ne soit nécessaire. Un état de fait déjà préoccupant qui, espérons-le, ne trouvera pas d'écho dans notre beau pays des droits de l'Homme et de la Liberté !



## Faible de sécurité majeure dans Netscape

Un des spécialistes de la sécurité de la Silicon Valley, Dan Brumleve (22 ans), a annoncé il y a quelques semaines sur son site avoir trouvé une faille majeure dans la sécurité de Netscape Navigator. Celle-ci permet d'accéder à l'intégralité des fichiers de l'ordinateur de la victime. Toutefois il est nécessaire que la victime se soit connectée à un site utilisant un applet Java spécifique, Brown orifice, qui exploite cette faille de sécurité et permet donc par la suite d'accéder au disque dur de la victime.

Dan Brumleve s'était déjà illustré fin 1998, en découvrant un trou de sécurité dans Netscape permettant de récupérer les cookies de la victime et donc de voir les derniers sites visités. [www.brumleve.com/BrownOrifice/](http://www.brumleve.com/BrownOrifice/)

## On ne plaisante pas avec ça !

Un internaute américain n'a rien trouvé de mieux que de menacer de faire exploser une école dans une chat room d'AOL. Cette menace aurait pu en rester là si un internaute ne l'avait pas signalé aux services de police dont dépendait l'école. Celle-ci à alors menée une enquête poussée remontant à un compte internet d'Indianapolis qui venait d'être piraté. Toutefois avec l'aide d'AOL et de l'opérateur de téléphonie BellSouth, le détective en charge de l'affaire, Gary Lowe, réussit à identifier le point de connexion original puis dans un deuxième temps, l'abonné ayant piraté le compte d'Indianapolis. En fait il s'agissait d'un adolescent de 15 ans qui suivait des cours à cette école...

# en bref l'actualité underground

## Démonstration de force

Lors de la "Black Hat" conférence organisée à Las Vegas, des centaines de spécialistes de la sécurité informatique ont pu assister à la démonstration de trois hackers qui ont piraté aisément l'un des produits de sécurisation réseau les plus importants du marché, Checkpoint Firewall-1. Ils ont ainsi mis en cause la sacro sainte croyance en l'invulnérabilité des firewalls.  
<http://www.checkpoint.com>

## I Love You, le retour !

Une nouvelle variante du tristement célèbre virus I Love You suscite actuellement toute l'attention du FBI; prénommée Love Letter, elle a touché des banques européennes et américaines au milieu du mois d'août. Sa spécificité résulte dans le fait qu'elle exécute un programme, hcheck.exe, permettant de récupérer des données confidentielles qui sont par la suite envoyées à trois adresses email, [ct102356@excite.com](mailto:ct102356@excite.com), [acch01@netscape.net](mailto:acch01@netscape.net) et [deroha@mailcity.com](mailto:deroha@mailcity.com). Ces données permettant d'accéder aux comptes bancaires en ligne, des personnes ayant reçu le virus. Oups !

## 007 n'a qu'à bien se tenir !

Sony innove une nouvelle fois avec un nouvel appareil photo numérique qui sera de la taille un paquet de chewing gomme pour un poids n'excédant pas les 26g. Doté d'une mémoire de type Memory Stick Duo de 64 Mo, il permettra le stockage de plusieurs centaines d'images (640 X 480 pixels.) Pour couronner le tout, il disposera d'un petit écran LCD de 1,4 cm. Aucune date ni aucun prix de commercialisation n'ont été indiqués.  
Source: L'Officiel du Net

## Une simple histoire de sex !

Enfin peut être pas aussi simple que cela et qui pourrait s'avérer extrêmement lucrative. L'histoire commence en 1994 avec l'enregistrement du nom de domaine "sex.com" par Gary Kremen. Quelques mois plus tard, il se rend compte que le nom de domaine a changé de propriétaire,

un certain Stephen Cohen.

C'est en 1997 que Kremen a décidé de porter l'affaire devant la justice; Il faut bien dire que les enjeux sont de taille puisque d'après Cohen sex.com générerait plusieurs millions d'euros par mois et le nom de domaine vaudrait plus de 250 millions d'euros. Dans son verdict la cour donna finalement raison à Stephen Cohen, mais de qui se moque t'on, je vous le demande...

## Cyber flicage en Chine

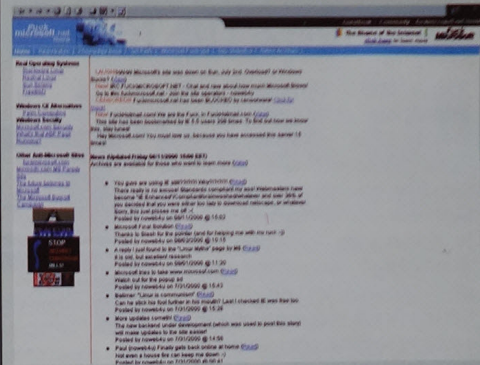
Tandis que leurs voisins taiwanais s'entraînent à la guerre électronique (cf news "Taiwan s'entraîne à la guerre électronique"), l'agence de presse "Chine nouvelle" a annoncé la mise en place dans une vingtaine de provinces et villes chinoises de structures de surveillance du Web. La première, celle de la province d'Anhui, aurait d'ailleurs déjà constaté et traité plusieurs infractions à la loi: détournements de fonds, pornographie, etc. Aucune mention n'étant faite d'infractions de type politique sur lesquelles le gouvernement chinois veille avec le plus grand soin en limitant l'accès de certains sites jugés non conformes aux intérêts chinois tels que les sites Web des médias occidentaux ou des organisations de défense des droits de l'Homme.  
Source: Chine nouvelle & Reuters

## Votez pour moi !

Nous savions que les Américains étaient avides d'argent mais je crois qu'ils réussissent une nouvelle fois à nous surprendre. Certains d'entre eux n'ont rien trouvé de mieux que de mettre leur bulletin de vote aux enchères sur le site eBay. Une de ces enchères ayant même atteint 700 FF! Comme quoi ils peuvent être cupides mais aussi stupides !

## Piratage téléphonique

Deux membres d'un groupe de phreakers (pirates téléphoniques) viennent d'être arrêtés par la police pour avoir diffusé des informations permettant le piratage de réseaux téléphoniques. Le préjudice s'élèverait à plus de 800 000 FF. Le site officiel cryptel.cjb.net n'est plus accessible mais nous avons pu constater la reprise sur d'autres sites des archives du site de Cryptel.



## Ils n'aiment pas beaucoup Billou !

Lorsque l'on parle de Microsoft, on peut être sûr de déclencher une polémique où vous trouverez des partisans acharnés de Linux comme des défenseurs de la société de Bill Gates. L'un des exemples les plus représentatifs est sans aucun doute le site Internet fuckmicrosoft dont le simple nom annonce d'emblée la couleur. Avec près de 9000 visiteurs par jour, ce site est un bon point

d'entrée pour découvrir toute une série de ressources en rapport avec la "résistance" anti-Microsoft et tout ce qui gravite autour.  
[www.fuckmicrosoft.net](http://www.fuckmicrosoft.net)

## Pervers pépère, Il n'y en a pas que pour les nazis !

Tandis que toute l'attention des médias et des internautes est obnubilée par l'affaire des objets nazis sur l'annuaire Yahoo!, d'autres personnes se régalaient de bienfaits du réseau mondial: Les pédophiles ! Ainsi dans le cadre d'une enquête anti pédophile, un américain de 49 ans, Myer Nevitt, a été appréhendé par la police pour possession et diffusion d'images pornographiques mettant en scène des enfants entre 11 et 18 ans. Pas moins de 300 disquettes auraient été saisies, des centaines de mégaoctets d'images... Cette arrestation fait suite à l'arrestation d'un autre pédophile américain, Wayne Camolli, qui animait un "ring" (réseau de sites) pédophile et une mailing list du même acabit.



# news, rumeurs, news, exclusif, news, brèves —>>> les Actualités

## Connexion illimitée, nouveau flop

OneTel était fier avant l'été de lancer son offre connexion illimitée (comprenant les télécommunications téléphoniques) pour 149 F par mois. Celle-ci se solda par un échec cuisant et son interruption brutale par l'opérateur téléphonique. C'est au tour d'AOL de se casser les dents sur ce type d'offre (99FF en connexion illimitée.) Difficile de croire que cette société n'avait pas prévu les ressources nécessaires, aussi peut-on se demander si cet échec n'a pas été prémédité avec comme objectif non avoué qu'un certain nombre des nouveaux abonnés conservent leur

abonnement malgré la suspension du forfait illimité. Une opération permettant ainsi de gagner plusieurs dizaines de milliers d'abonnés très rapidement.

Que ce soit OneTel ou AOL, les internautes sont traités avec un mépris tout à fait édifiant. Les fournisseurs d'accès les considèrent comme une simple marchandise à laquelle l'on applique tel ou tel traitement en fonction des besoins et des objectifs mercantiles fixés.

Il n'y a pas à dire, le temps de l'Internet libre et indépendant s'éloigne à grand pas, laissant la place aux marchands.

[www.adim.asso.fr](http://www.adim.asso.fr)

## Querelle de voisinage en ligne !

Imaginez une querelle de voisinage qui dure depuis trois ans à propos de la construction d'un garage; un hollandais qui se voit diffamé par son voisin dans la presse locale afin de l'empêcher de construire son garage qu'il considère comme trop près de sa maison. Voici le contexte de l'affaire. Vous vous demandez toujours quel rapport

avec la choucroute ? Et bien l'un des voisins a décidé de prouver son bon droit en plaçant une webcam qui pointe en permanence sur son garage en construction. Vous allez pouvoir espionner en toute tranquillité l'évolution du chantier et les éventuels sabotages !

<http://www.deslechteadem.com>

## Piratages en série en Roumanie pour les élections

Tandis que la campagne électorale battait son plein en Roumanie, les sites Web de plusieurs personnalités politiques de premier plan ont subi les assauts répétés de pirates informatiques. Ceux-ci redirigeaient les visiteurs vers d'autres sites qui n'avaient que peu de rapport avec les originaux. Ainsi le site officiel de l'ancien président Ion Iliescu redirigeait vers la page du FBI sur laquelle figurent les criminels les plus recherchés. Une semaine auparavant c'est vers un site pornographique français que

l'adresse avait été "reroutée". Dans le même esprit, le site de l'ancien Premier ministre Theodor Stolojan avait été redirigé vers le site de la présidence roumaine. <http://www.ioniliescu.com>



## Du nouveau dans la localisation des internautes

Une petite révolution serait-elle en passe d'être franchie dans le monde de la détection géographique en ligne. En effet, une start-up basée à Mountain View (Californie), Quova Inc., aurait trouvé le moyen de localiser les internautes et de proposer, notamment, des publicités ciblées. Ainsi des sites marchands pourront proposer des casquettes du PSG aux internautes parisiens et des Tee Shirts de l'OM à ceux se connectant depuis Marseille.

Quova utilise les techniques de pings, d'adresses IP et de traceroute pour localiser les points de connexion et, par la suite, vérifie tous les jours si ceux-ci sont toujours valables. Sur les six derniers mois pas moins d'une centaine d'administrateurs réseaux se sont toutefois plaints auprès de la société.

<http://www.quova.com>

## Il avale tout !

Carnivore, le système de surveillance développé par le FBI serait bien plus qu'un simple logiciel de contrôle de courrier électronique. C'est en tout cas la conclusion que l'association EPIC (Centre d'Information sur la Confidentialité Electronique) après examen des quelques documents techniques que le FBI avait dû donner suite à une décision de justice. L'EPIC ajoute que Carnivore ne se limiterait pas à un simple filtrage des emails de personnes sous surveillance mais serait capable d'enregistrer l'ensemble des données véhiculées via le serveur où il est présent (Carnivore s'installe sur les serveurs des fournisseurs d'accès Internet). Des informations encore non vérifiées qui attendent d'être confirmées par l'examen d'autres documents...

[http://www.epic.org/privacy/carnivore/foia\\_documents.html](http://www.epic.org/privacy/carnivore/foia_documents.html)

## On a ne rigole plus !

Il faut croire que quelque chose ne tourne vraiment pas rond dans la taille des sujets britanniques. Peut-être un effet secondaire de la vache folle ? Après que certains journaux à scandale aient publié les photos, noms et adresses de dizaines de pédophiles résidant en Angleterre, c'est au tour des écossais de prendre ce genre d'initiative mais cette fois, via un site Internet.

Le responsable de cette "glorieuse" opération, Stuart Carnie, est le leader de l'association «Freedom for Children» qui entend ainsi «couvrir de honte» les pédophiles.

Rappelons que la vindicte populaire avait entraîné des actes de violences contre des innocents.

Source: AFP

Tous les trois mois, retrouvez toute l'actualité alternative dans Hacker News Magazine

# en bref l'actualité underground

**On a cru que Bill n'était plus l'homme le plus riche du monde !**

Drôle d'aventure que celle de ce norvégien qui est devenu l'espace de quelques jours l'homme le plus riche du monde. C'est en effet en consultant son compte bancaire via Internet qu'il a remarqué que son compte était crédité de 9 999 999 973 885 24 couronnes norvégiennes (environ 6,5 milliards de francs.) Il l'a signalé à sa banque qui ne s'explique toujours pas cette erreur.

Source: AFP

**En veux-tu ? en voilà.**

Un hacker se faisant appeler Pimpshiz aurait en quelques semaines piraté plus de 60 sites Internet utilisant Windows NT comme système d'exploitation. Parmi les sites touchés, celui de la bibliothèque de France et de la Nasa (Houston nous avons un problème!). Le pirate informatique entend protester contre le traitement que subit la société éditrice de Napster (procès en cours)

<http://www.bnf.fr>

**Trop fort le patch !**

Le premier Service Pack pour Windows 2000 a eu des conséquences surprenantes. Le patch, qui faisait plus de 83 Mo, a en effet eu comme conséquence de rendre inefficaces certains logiciels réseau de protection tels que BlackIce ou ZoneAlarm. Les sociétés éditrices de ces firewalls ont à leur tour mis à disposition des patches correctifs du patch Microsoft !

<http://www.netice.com>

<http://www.zonelabs.com>

**Le téléphone portable nuie à votre santé !**

Comme tous les jours, Noel Connely, jeune Londonnien de 38 ans, téléphonait de bon matin pour profiter des heures creuses. Comme tous les matins il se penchait à son balcon pour avoir une réception optimale, mais cette fois ci il est tombé et a trouvé la mort. Le mois dernier un homme a été grièvement blessé dans un zoo mexicain en essayant de récupérer son téléphone cellulaire tombé dans la cage du lion. Le téléphone s'était

mis à sonner et avait réveillé l'animal !

**Des Hollandais à l'écoute**

Les services secrets hollandais, BVD, auraient mis en place un logiciel de surveillance du courrier électronique. Ce logiciel aurait été expérimenté une première fois dans le cadre d'une surveillance à l'encontre d'une société traitant avec l'Iran.

<http://www.minbzk.nl>

**Le crime ne paie pas**

Trois escrocs qui avaient acheté une base de données incluant plus de 3 millions de numéros de carte de crédit viennent d'être condamnés à payer plus de 260 millions de francs d'amende pour avoir débité abusivement de l'argent pour de prétendues visites de sites Web adultes.

**Ca peut coûter cher**

Un webmaster ayant placé des liens sur ses pages HTML vers des sites proposant des albums musicaux / fichiers MP3 pirates, vient de se voir condamné à 20 000 FF d'amende et à 4 mois de prison avec sursis. Comme quoi il faut faire attention vers où pointent vos liens hypertextes.

**Les pirates dans la course à la présidence**

Des sites Web proches du Parti Républicain et Démocrate ont subi les assauts répétés de pirates la veille et le jour du scrutin, le 7 novembre dernier. Elles ont aboutis à la fermeture des sites Web attaquées.

<http://www.rnc.org>

<http://www.dnc.org>

**Silence, on tourne !**

Un jeune homme n'a rien trouvé de mieux que d'essayer de pirater le film "The Watcher" en le filmant avec son caméscope lors d'une séance à Enghien. Interpellé par la police après avoir été expulsé du cinéma, il risque 10 000 FF d'amende pour avoir violé la propriété artistique.

Source: Le Parisien



**Walker Texas Ranger ?**

**NON**

**Hacker Texas Ranger !**

Un peu à l'image de ce que viennent de faire les Chinois, les Texans ont mis sur pied une unité de police ayant pour tâche la surveillance et la répression des délits en ligne. Composée de 20 agents, elle a déjà permis le démantèlement de trafic de drogue, de logiciels piratés, d'espionnage industriel et d'un réseau pédophile important.

**L'école fliquée**

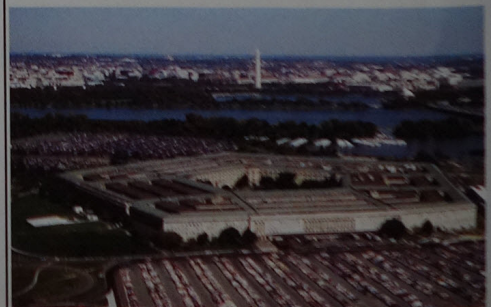
Suite à la demande d'un parent d'élève américain, James M. Knight, une cour de justice a décidé d'autoriser la publication et diffusion de la liste des sites Web visités par les étudiants sur les ordinateurs de l'école.

Source: NYT

**Arrêtez, par pitié...**

Cité par Reuters, le directeur de la sécurité du Pentagone a supplié le 8 août dernier les pirates informatiques d'arrêter de s'en prendre aux systèmes informatiques. Il faut dire que les attaques ont été multipliées par presque quatre entre 1998 et 1999 pour atteindre 22 000 l'année dernière. Elles devraient dépasser les 25 000 cette année.

[www.defenselink.mil](http://www.defenselink.mil)



# news, rumeurs, news, exclusif, news, brèves —>>> les Actualités

## Ca rigole et ca tchatte bien en interne à la CIA !

La CIA nous réserve décidément beaucoup de surprises; nous apprenons ainsi que certains de ses employés auraient placé une chat room secrète sur les serveurs de l'agence de renseignement américaine où plus de 160 salariés se retrouvaient pour discuter de choses et d'autres, pour se raconter des blagues ou tenir des propos pas toujours du meilleur

goût. Le pôt aux roses a été découvert lors d'un contrôle de sécurité de routine. Les salariés ayant enfreind les règles de sécurité de la CIA risquent une mise à pied et pour les initiateurs de la chat room, un licenciement pur et simple. Ca ne rigole pas au pays de l'Oncle Sam !



## Cyber unité policière: 250 millions de francs alloués

Les Anglais se donnent manifestement de gros moyens pour lutter contre la pédophilie, la fraude et le racket en ligne. A partir du mois d'avril prochain, ce sont pas moins de 80 policiers qui seront détachés à plein temps pour combattre la cyber criminalité naissante. Ils seront pour moitié basés sur Londres et

pour l'autre moitié dispatchés au niveau local. Le secrétaire d'Etat, Jack , a déclaré que "le gouvernement (anglais) est décidé à agir contre la criminalité high Tech dans le but de faire du Royaume Uni l'endroit le plus sûr du monde pour conduire et démarrer dans l'eCommerce.

## La version pakistanaise de l'avion espion **EXCLUSIF**

Les gardes frontière indiens ont eu la surprise de capturer le premier "avion" espion pakistanais: un faucon équipé d'une minuscule antenne et d'un transmetteur radio !

Il va sans dire que la provenance de ce faucon est supposée être le Pakistan mais rien ne permet de l'affirmer de façon certaine... Depuis le début de l'année, c'est

le troisième faucon qui est ainsi capturé à proximité de la frontière entre l'Inde et le Pakistan. Deux pays qui se sont à trois reprises depuis 1947.

Comme quoi, on peut parfois être surpris des applications faites de la technologie. Trop forts ces Pakistanais !

Source : Reuters

## Piratage en culotte courte

Il n'y a déjà pas d'âge pour s'amuser ! C'est sûrement ce que se sont dit deux étudiants d'un collège de Lexington (Kentucky) en piratant les ordinateurs de leurs professeurs et en faisant tomber l'ensemble du réseau pendant une demi heure. Aucune information concernant les 1800 étudiants n'a toutefois

été perdue ou dérobée mais tout ceux qui travaillaient sur leurs ordinateurs au moment du crash ont tout de même vu leur travail disparaître...

Une fois les deux pirates identifiés, les sanctions ne se sont pas faites attendre avec une expulsion immédiate de 10 jours.

## Une version spéciale "Start Up" du Monopoly

La société Hasbro, éditrice du Monopoly, vient de mettre en vente une version spéciale du célèbre jeu de société. Vous n'y retrouverez donc plus Rue de la Paix, Gare St Lazare ou Bld St Michel mais Yahoo!, eBay ou Excite.

Prénomée la "Dot Com Edition", elle permettra à tous les passionnés de la nouvelle économie de s'amuser tout en restant en contact direct avec les plus importants acteurs de l'Internet.

Pour l'instant uniquement en anglais, la version française de ce Monopoly n'est pas encore prévue. Comme toutefois

le Web est international, vous ne serez pas trop dépayés ! Une initiative amusante et intéressante qui fera une bonne idée de cadeau.



<http://www.hasbro.com>

## Microsoft Office 10 Qui dit nouvelle technologie, dit floraison de bogues !

Mi novembre, la société de Bill a distribué la deuxième version beta de sa suite bureautique, Office. Très proche au niveau ergonomique des précédentes version, la version 10 devrait toutefois intégrer toute une série de nouvelles technologies développées par Microsoft. Si l'on fait fi des patches de sécurité pour Outlook et de l'intégration de la reconnaissance vocale, nous vous citerons la technologie nommée ".Net" qui permettra une plus grande interpénétration entre la suite bureautique et Internet.

Autant vous dire que les failles de sécurité ou bogues en tout genre devraient être légion dans cette nouvelle version qui sera commercialisée l'été prochain. Nous ne manquerons pas de revenir sur ce point dans un prochain numéro de Hackers News Magazine.

## A la trace...

L'Inde vient de voter une loi anti-pirate, probablement à la suite de l'affaire "I Love You" dont l'auteur philippin avait bénéficié d'un vide juridique dans son pays. Dans la foulée, le principal opérateur indien vient d'annoncer qu'il garderait toutes les traces des connexions de ses abonnés. Source: Zataz

# en bref l'actualité underground

## Spam contrôleur

Un journaliste de Libération nous faisait découvrir début novembre un service bien utile pour lutter contre le spam (courrier électronique non sollicité le plus souvent de nature publicitaire.) Ainsi en s'inscrivant sur le site SpamCop (gratuit), l'internaute peut télécharger un petit programme qui analyse ses emails et retrouve la trace de l'envoyeur. Puis il enverra au nom du "spammé" un rapport à son fournisseur d'accès Internet. Dans la plupart des cas celui-ci déconnectera les comptes des spammeurs.

<http://www.spamcop.net>

## eBay: oui aux enregistrements pirates !

Les décisions de justice se suivent mais ne se ressemblent manifestement pas beaucoup. En effet, eBay a obtenu du juge Stuart Pollack le droit de laisser ses utilisateurs vendre des enregistrements audio piratés. Le juge a ajouté que «la tentative de plaignant d'imposer à eBay la responsabilité des objets mis en vente sur son site n'est pas différente de la tentative infructueuse qui voulait faire des anciens fournisseurs d'accès des éditeurs plutôt que des distributeurs.» (les rendant ainsi responsables des contenus des sites qu'ils hébergent).

Dommage que la justice ne soit pas plus proche de cette vision des choses.

## Pas si secret ces Suisses

Les virements, les adresses et les numéros de comptes de clients, pour la plupart des vedettes du show business, sont apparus sur le site Web de la banque Credit Suisse au vu et au su de tout le monde. Le système de sécurité du site ne serait pas directement concerné et cette erreur résulterait d'un tiers qui aurait publié les informations sur ces 650 personnes au mauvais endroit. Certains clients s'apprêteraient à porter plainte.

<http://www.credit-suisse.com>

## Espionnage de courrier

La justice européenne n'est décidément pas très uniformisée comme ont pu le constater à leur

sdépends trois gestionnaires de l'Ecole Supérieure de Physique et de Chimie Industrielle. Ceux-ci ont en effet été condamnés à 10 000FF d'amende pour avoir espionné le courrier électronique d'un de leur étudiant. Une décision à mettre en vis à vis de la nouvelle législation anglaise permettant aux entreprises anglaises de surveiller comme bon leur semble les communications électroniques privées de leurs salariés.

<http://www.espci.fr>

## Le GPS, version européenne

L'agence européenne ESA a présenté la version "made in Europ" des systèmes GPS (américain) et Glonass (Russe); Egnos devrait permettre de localiser quelqu'un avec une précision de l'ordre du mètre pour le GPS et une soixantaine pour Glonass. Le dispositif opérationnel en 2003 sera, espérons-le, utilisé à bon escient !

<http://www.esa.int/navigation/>

## Pirate "maître" chanteur

Il ne manque décidément pas d'humour! Le pirate hollandais ayant réussi à pirater les serveurs de Microsoft n'a rien trouvé de mieux que de demander à ce que la chanteuse Britney Spears lui téléphone en échange de ses informations.

## Navidad, le virus espagnol

En l'espace de quelques semaines un nouveau virus, Navidad (ndlr: Noël en espagnol), s'est attaqué à plus d'une dizaine de gros sites japonais. Il aurait causé des dommages importants qui n'ont pas encore été évalués.

Source: Japanese Center for Information Technology Security (CSTI)

## 7 nouvelles extensions

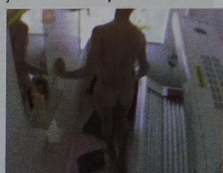
L'organisme de contrôle d'Internet, l'ICANN, vient de décider de créer 7 nouvelles extensions pour les noms de domaine qui s'ajouteront au ".com", ".net" etc. existant.

Vous pourrez donc dès l'année prochaine avoir un nom de domaine se terminant par ".biz" (business), ".info", ".pro" (professionnels), ".museum", ".aero" (voyages), ".name" et ".coop". On pourra s'étonner que des extensions telles que ".web" ou ".sex"

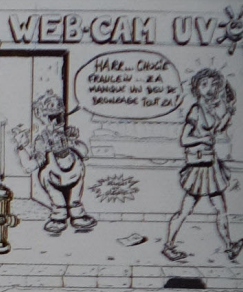
# SPECIAL ALLEMAGNE

## Malin comme un allemand...

Manuel Scholz est ce que l'on pourrait appeler un petit malin. Il vient de proposer des séances gratuites aux clients acceptant d'avoir une webcam dans leur cabine UV. Nous l'avons testé et ça marche plutôt bien



M. Scholz espère que la publicité assurera la rentabilité du concept. [www.gratis-solarium.de](http://www.gratis-solarium.de)



## Riche comme un allemand...

Imaginez un peu... Vous êtes en vacances et lorsque vous revenez vous apprenez que vous avez gagné plus de 60 millions de francs ! C'est ce qui vient d'arriver à un allemand qui a joué au loto le 5 août dernier puis est parti en vacances sans attendre les résultats. Lors du tirage du 12

août, c'est le jackpot, 10,2 millions d'euros ! N'ayant pas pu être contacté, la somme lui a toutefois été versée sur son compte bancaire, il était en effet abonné au loto. Comme quoi les retours de vacances peuvent être parfois agréables ! Source: AFP

## Méchants comme certains allemands...

C'est après le dépôt du nom de domaine "heil-hitler.de" par une organisation néo nazie que la ministre allemande de la justice, Herta Daeubler Gmelin, a déclaré vouloir faire en sorte que ce type de noms de domaine soient purement et simplement interdits. Elle a par ailleurs ajouté que ces noms de domaine

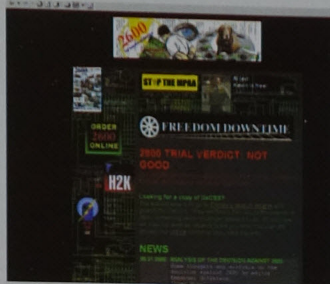
pourraient pointer vers des pages d'information antiracistes.

Les organisations antiracistes américains utilisent déjà cette façon de faire, un espace de cybersquatting pour la bonne cause. Pour info, le site heil-hitler.de a été fermé, bien sûr... Et Dieu merci ! Source: AFP

# news, rumeurs, news, exclusif, news, brèves ->>> les Actualités

## Dans la finesse !

**verizon** L'opérateur téléphonique américain Verizon a dépensé plus de 50 000 \$ (environ 365 000 FF) pour déposer pas moins de 707 noms de domaine. Parmi ceux-ci verizonstinks.com (traduction littérale: verizonpue.com) et toutes les variantes que vous pouvez fort aisément imaginer... Un magazine underground, 2600, a donc décidé par provocation de déposer le nom verizon-REALLYstinks.com (traduction: verizonpuevraiment.com). En réponse, Verizon menaçait de poursuivre le responsable de la publication qui refusa de céder et enfonce encore le clou en déposant verizonshouldspendmoretimefixi



ngitsnetworkandlessmoneyonlawyers.com (traduction littérale: verizondevraitpasserplusdetempsàvérifiersesserveursetmoinsd'argentavecseavocats.com) Une affaire que nous ne manquerons pas de suivre !  
<http://www.verizon.com>  
<http://www.2600.com>

## Le racisme sur internet : une fatalité ? Non !

La ministre française de la Justice, Marylise Lebranchu, a affirmé que la répression de la cybercriminalité devait également viser les délits de racisme, de xénophobie et d'antisémitisme, lors d'un colloque sur internet organisé par la Ligue internationale contre le racisme et l'antisémitisme (LICRA). La ministre a regretté qu'en l'état actuel de sa rédaction, le projet européen de loi ne comporte pas de dispositions sur les infractions racistes ou antisémites commises par la voie de l'internet. "La France

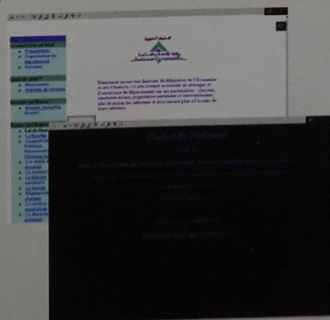
n'accepte pas cette orientation et elle s'est tout récemment fortement exprimée en ce sens", a-t-elle rajoutée. "Nous recherchons activement le soutien des autres pays de l'Union européenne sur ce point".

Mme Lebranchu pourra en tout cas compter sur la communauté underground et plus spécifiquement des pirates informatiques qui ont souvent montré leur engagement contre le racisme en ligne avec le piratage de sites racistes comme celui du Ku Klux Klan.

## Maroc : Le ministère des finances piraté !

Le site Internet du ministère de l'économie et des finances marocains a vu sa page d'accueil remplacée par une belle page noire avec un petit texte expliquant le pourquoi du piratage. La page a été tout simplement remplacée sans aucun autre préjudice dommageable. Comme quoi il y a des pirates pas trop méchants qui peuvent rester sympathiques !

<http://www.mfie.gov.ma>



## Documents secrets: Nixon, le meilleur copain de Pinochet

Décidément les américains nous réservent surprises après surprises. Des documents issus des archives secrètes viennent ainsi d'être publiés sur Internet où les internautes peuvent découvrir le rôle actif du gouvernement dans le renversement de la démocratie chilienne en 1973 au profit d'une dictature militaire conduite par le général Pinochet. On peut notamment y lire cette phrase du Président Nixon : «faire tout ce qu'il est possible de faire pour descendre Allende» («do everything we can to bring Allende down»)

C'est le Président Clinton qui a autorisé l'ouverture de certaines archives concernant cette époque à la suite de la pression de certaines organisations qui enquêtaient sur le projet Condor. Un projet concernant l'ensemble des régimes dictatoriaux d'Amérique du sud qui avaient travaillé ensemble pour éliminer leurs ennemis respectifs.

Peter Kornbluh du groupe de recherche National Security Archive (université Washington) explique «qu'à la lumière de ces documents, l'histoire de l'intervention américaine au Chili et de la dictature de Pinochet peuvent être réécrites. Ils fournissent des éléments d'un grand intérêt pour les historiens, mais également pour les cours de justice qui auraient à juger ceux qui ont commis des atrocités durant la dictature de Pinochet »...

<http://www.gwu.edu/~nsarchiv/news/20001113/>  
Source : ZDnet

## Microsoft hacké, C'est reparti !

En l'espace de quelques semaines, les serveurs de Microsoft ont subi deux piratages importants. Le dernier en date résulterait d'un patch correctif non installé sur le serveur Internet Information Server (IIS). Le pirate aurait ainsi accédé à plusieurs sites et placa un petit fichier texte "Hack The planet". plus inquiétant, le pirate a déclaré être en mesure d'altérer des fichiers sur les serveurs de téléchargement de Microsoft. Espérons que cela soit du bluff car si les logiciels de Microsoft sont vérolés en plus d'être bogués, c'est pas gagné...

## I Love You, le retour ?

Une nouvelle variante du tristement célèbre virus "I Love You" a touché une petite ville des Etats Unis, Ogden. Il se présente comme un fichier joint (jusqu'à présent rien de nouveau) de type image ou HTML, et là c'est nouveau et dangereux. On a en effet plus tendance à ouvrir une image jointe qu'un fichier avec une extension "VBS" comme c'était le cas pour "I Love You". Le virus efface ou renomme les fichiers de l'ordinateur infecté...



## Le rassemblement underground de l'été

C'est du 28 au 30 juillet dernier qu'a eu lieu à Las Vegas, le plus grand rassemblement de pirates informatiques de la planète. Pour cette huitième édition du Defcon, tout le gotha du milieu underground était présent et y côtoyait la fine fleur des services de sécurité ou secrets de plusieurs pays avec toutefois une majorité d'américains (NSA, FBI, etc.) Parmi les interventions les plus attendues, celles de **Benneth Haselton**, de **Ian Vitek** et **Ian Goldberg**.

Plus de 5000 visiteurs ont assisté à la convention dans une ambiance toute particulière où les jeunes "boutonneux" aux cheveux verts et pratiquant le piercing se sont étonnés de voir autant de jolies filles (mannequins embauchées pour orienter les visiteurs ou pour faire de la promo.) Un véritable succès qui a drainé toute l'intelligentsia américaine que l'on retrouvait le soir dans les casinos et dans les boîtes à striptease... Une édition 2000 sage et un brin ennuyeuse qui, si nous devons la noter, recevrait 10/20 ■

### Les intervenants

#### Benneth Haselton - Peacefire

Eminence des méthodes de blocage en ligne (Firewall, logiciel de censure), il expliqua devant une assemblée conquise un nouveau protocole basé sur la stéganographie pour contourner l'interdiction d'accéder à certains sites du fait de firewall présent dans de nombreuses entreprises. Assez complexe !

<http://www.peacefire.org>  
**Ian Vitek - Infosec**

Spécialiste suédois de l'intrusion, Ian Vitek a dévoilé ses dernières trouvailles en matière de piratage informatique. Son exposé sous forme de pas à pas a démontré la possibilité de contourner un firewall après le piratage d'une adresse IP, le tout sous Linux.

<http://www.infosec.com>

#### Ian Goldberg - Zero-Knowledge Systems

Bientôt diplômé de l'université de Berkley, Ian Goldberg a fait le point sur le logiciel "Freedom" devant assurer l'anonymat des internautes sur les différents protocoles d'accès à Internet (WWW, email, IRC, etc.) Il s'est illustré de part le passé en dévoilant des failles de sécurité dans le protocole sécurisé SSL et dans les algorithmes d'encryption des téléphones portables GSM. <http://www.freedom.net>

#### David J. DiCenso - SecureLogix Corporation

Ancien instructeur militaire spécialisé dans la législation informatique, David J. DiCenso a débattu sur un thème de plus en plus d'actualité: "Le citoyen Hacker: Patriote ou criminel de guerre ?".

On peut en effet se demander à partir de quand le piratage informatique à l'échelle internationale devient un "acte de guerre?" Certains parmi la communauté des Hackers pensent que le DoD (Department of Defense) gère mal le piratage international, qui serait plus efficacement opéré si laissé aux experts-les hackers "civils". Ce point de vue est intéressant, mais est-il approprié ? Quelles sont les implications au niveau international des opérations sur le réseau électronique, dont la cible sont des personnes ou des états étrangers? Jusqu'où un informaticien peut-il aller sans que ses actes ne deviennent des "actes de guerre?" Quelles représailles un état ciblé a-t-il le droit d'organiser selon les lois et les conventions internationales? Quelles règles s'appliquent ? Dans un monde où les hackers sont assez téméraires pour déclarer la guerre à des états détenteurs d'armes nucléaires, où les états organisent des opérations véritablement "militaires" contre des civils dans d'autres états qui ne sont pas hostiles, ces problèmes épineux sont de la plus haute importance. Cette présentation fut l'occasion d'aborder ces problèmes, dans un effort de mettre en lumière cette problématique forte qui se fait de plus en plus présente dans les relations internationales. Les débats furent houleux et passionnés et les avis vraiment partagés.

<http://www.freedom.net>

<http://www.defcon.org>

Le plus grand salon annuel du milieu underground.



JULY 28-30 2000  
LAS VEGAS NV



# Regardez ce que vous voulez quand vous voulez !

La télévision à la carte : un rêve qui devient aujourd'hui réalité avec l'apparition sur le marché américain de magnétoscopes étonnants : les Personal TV (PTV).

L'étrange lucarne posée dans nos salons a toujours fait l'objet de nombreuses prospectives. Depuis quelques temps on souhaite la marier à Internet, pour mieux servir le téléspectateur et le combler au niveau de ses choix télévisuels à l'heure où il le désire. C'est ce que l'on a appelé, à l'image de " l'ordinateur personnel " (PC, ou Personal Computer) la " télévision personnelle " (PTV, Personal TV). Mirage ou virage ? En tous cas, parmi les tentatives les plus farfelues pour forcer ce mariage, une machine étonnante pourrait bien faire figure de précurseur. En effet, pour mettre en route cette télé personnelle, plusieurs constructeurs, commencent à inonder le marché américain avec des appareils révolutionnaires. Des magnétoscopes étonnants que l'on nomme DVR (Digital Video Recorder), PTV Box (Personal Television Box) ou aussi HDR (Hard Drive Recorder).

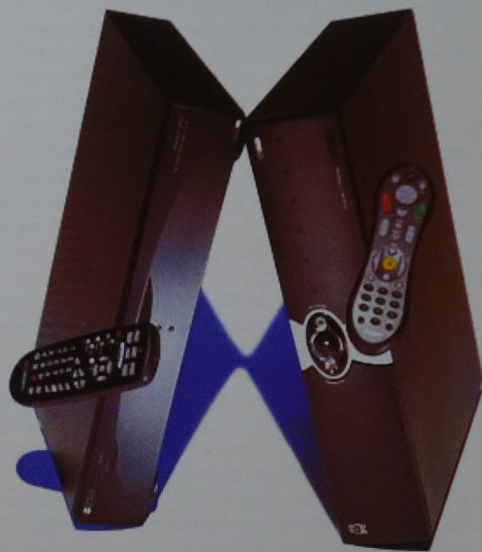
Ces magnétoscopes numériques vont certainement entraîner une véritable révolution dans la façon de regarder la télévision. Ces appareils de nouvelle génération coûtent 400 dollars (soit environ 2400 francs). Un enregistreur PTV est un appareil ressemblant à n'importe quel magnéscope VHS. D'ailleurs, il se branche, tout comme lui, au téléviseur, via la prise Peritel. Il exploite n'importe quel canal de réception, que ce soit une antenne hertzienne, un décodeur câble ou satellite. A l'intérieur du PTV, on trouve un certain nombre de composants électroniques qui rappellent curieusement ceux d'un ordinateur. Tout d'abord, un processeur PowerPC, que l'on retrouve habituellement dans les Macintosh, des convertisseurs analogique-numérique, nombre de connecteurs pour brancher le magnéscope à différentes sources (connectique S-Video, etc...) et un véritable système d'exploitation pour

mettre en œuvre l'ensemble. Il s'agit essentiellement d'un noyau de Linux. Enfin, l'élément le plus étonnant : un gros disque dur d'une capacité allant de 15 et 30 Go (voire 60 Go pour un modèle à venir) selon les modèles. Il s'agit dans la plupart des cas d'un disque dur Quantum prévu à cet effet : le I.link. Pour numériser les images, cela se passe comme sur n'importe quel ordinateur. Le format de compression est le Mpeg-2. Ainsi, avec ce système, sur un modèle de 25 Go, l'appareil peut conserver jusqu'à 30 heures de programmes en mode standard, c'est-à-dire avec une qualité légèrement supérieure à celle d'un magnéscope analogique actuel. En optant pour une qualité proche de celle d'un DVD, on descend à moins 20 heures, ce qui reste tout de même très correct. Lorsque le disque dur est rempli, il suffit d'une pression sur un des boutons de la télécommande pour supprimer instantanément les émissions que

vous ne souhaitez pas conserver. Vous pouvez tout aussi bien définir des priorités afin que le système efface lui-même les programmes que vous jugez les moins importants quand il a besoin de place. Et lorsque vous désirez conserver un bon film, une prise sur l'appareil est prévue pour y raccorder votre magnéscope et faire une copie du film sur une cassette VHS.

Toutefois, le PTV ne se limite pas à un simple magnéscope doté d'un gros disque dur et faisant fi de cassettes vidéos. Tout comme sur un lecteur de DVD, il n'y a pas de rembobinage et on peut accéder de façon instantanée à n'importe quel point du film ou de l'émission. Cela permet, une fois qu'on maîtrise les secrets d'une télécommande assez spéciale, d'effectuer un arrêt sur image, un défilement image par image ou un retour en arrière immédiat pour revoir un passage au ralenti. Et surtout de mettre en pause un

film ou un programme en cours de diffusion (c'est à dire qui n'est pas enregistré mais bel et bien diffusé) pour le reprendre à l'instant où vous l'avez laissé. Prenons un exemple : Le téléphone sonne durant votre émission préférée ou encore, une envie pressante vient poindre au moment crucial d'un film poignant. Comme sur n'importe quel magnéscope, il suffit d'appuyer sur pause pour suspendre la diffusion. Mais c'est ici que s'arrête la comparaison ! En effet, une autre pression sur cette touche " pause " et on reprend le programme à l'instant précis où on l'a quitté. En effet, pendant cette interruption, le magnéscope a continué à enregistrer ce que vous avez manqué. Une performance autorisée par la capacité qu'a un disque dur à "lire" et "écrire" simultanément. Pratique pour ne pas louper une miette de la Coupe du monde, mais avec une conséquence logique : un léger différé.



# REGARDEZ CE QUE VOUS VOULEZ QUAND VOUS VOULEZ !

NUMÉRIQUE

Mais les perspectives offertes par l'appareil sont encore bien plus spectaculaires. Car la principale qualité de l'enregistreur PTV est de libérer le téléspectateur de la contrainte horaires. Ainsi, vous pouvez choisir à l'avance les programmes que vous désirez enregistrer par une simple pression sur un bouton de la télécommande et même laisser l'appareil se faire une idée de vos goûts et habitudes grâce à des touches spécifiques intégrées à la télécommande. Celles-ci sont symbolisées par un pouce : pouce vers le haut (on aime) et pouce vers le bas (on n'aime pas). Avec certains modèles, vous pouvez aussi enregistrer une émission sur une chaîne pendant que vous en regardez une autre. Vous disposez ainsi en permanence d'un stock de programmes dans lequel vous pouvez puiser quand vous le voulez. En bref : une télé à la carte. Mais attention, cette performance n'est pas possible à l'aide du seul enregistreur PTV. Il faut que celui-ci ait pris connaissance des programmes TV, des horaires et de bon nombre d'informations sur les canaux que vous utilisez. C'est là qu'Internet joue son rôle, grâce à un petit modem embarqué et branché sur votre ligne téléphonique. Selon votre modèle de magnéscope, celui-ci va se connecter via Internet aux serveurs d'une des deux sociétés ayant la primeur sur cette télévision de demain : TiVo et Replay Network. Ici, il peut piocher sur toutes les chaînes les programmes répondant à vos goûts spécifiques. L'ensemble est stocké sur le disque dur (jusqu'à trente heures) et recompilé dans l'ordre désiré. Le téléspectateur peut ainsi se faire un petit menu télévisuel débarrassé de publicité ou de toute autre interruption. A cet usage, certains modèles possèdent même une touche spécifique permettant d'aller 30 secondes plus loin. Bien sûr, il est aussi possible de se connecter soi-même pour effectuer ses propres réglages, mais aussi pour bénéficier de services en ligne annexes, dont le courrier électronique. Le PTV permet en effet de recevoir et d'envoyer des e-mails. C'est ainsi que la télévision personnelle est née, entraînant peut être à terme la mort des chaînes de programmes traditionnelles.

Louis Neveu

## NOUVEAUTE

Alors que nous terminions d'écrire cette article sur les magnétoscopes numériques, Toshiba a annoncé la sortie de son magnéscope numérique pour la fin décembre au Japon. Il combinera un disque dur de 30 Go et un lecteur/enregistreur DVD-RAM. 33,5h pourront être enregistrées grâce au Toshiba RD-2000

[www.toshiba.co.jp/about/press/2000\\_11/pr1601.htm](http://www.toshiba.co.jp/about/press/2000_11/pr1601.htm)

## Les modèles de magnétoscopes numériques déjà disponibles

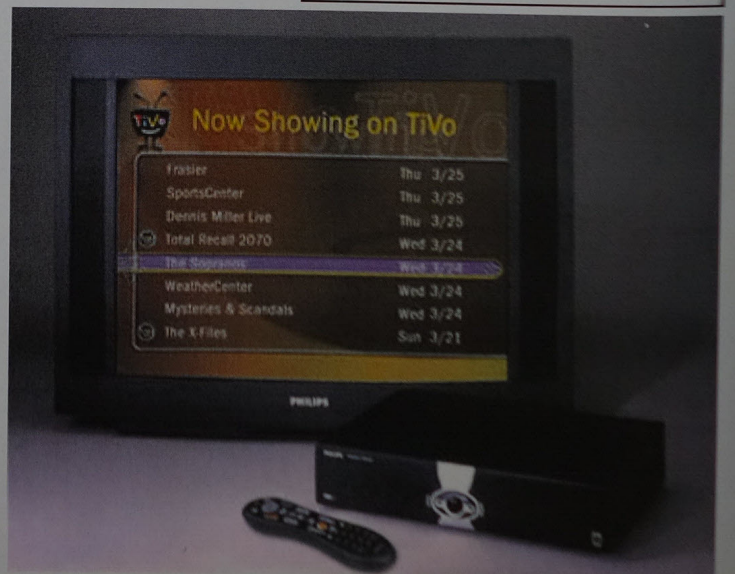
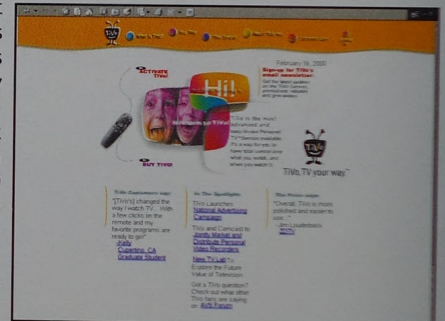
Depuis quelques mois, les principaux modèles de PTV sont disponibles uniquement aux Etats-Unis. Même si pour l'instant les ventes sont encore marginales (en 1999, Philips aurait, selon TiVo, réussi à écouler 26 000 magnétoscopes numériques), les sociétés d'études de marché comme IDC annoncent le chiffre astronomique d'un million d'appareils vendu pour l'an prochain. Les mois futurs seront donc rythmés par l'annonce de nouveaux modèles de PTV et de nouveaux acteurs dans ce marché émergent. Pour le moment, seuls deux modèles rencontrent un succès croissant. Il s'agit des modèles de TiVo et de ReplayTV. Leur prix se situe aux alentours de 2800 et 4200 francs et leur principal point fort tient à leur simplicité d'utilisation et leurs fonctions étonnantes.



### TiVo

Avec le TiVo, l'utilisateur doit s'abonner au service en ligne quotidien (10\$ par mois, ou 99 \$ par an et près de 200 \$ pour une concession à vie !). Le magnéscope se connecte automatiquement à une heure précise sur le serveur de TiVo via Internet pour mettre à jour les informations concernant la programmation. Le modèle de TiVo est commercialisé sous plusieurs marques, avec le Philips HDR112 et HDR312 et le Sony SVR-2000. Les magnétoscopes de Philips disposent d'un disque dur Quantum d'une capacité de 14 ou 30 heures. Dans le cas d'une mémorisation de programme avec une haute définition, cette capacité n'est plus que

d'environ 18heures. Enfin, tout comme un ordinateur, le PTV de Philips possède son propre système d'exploitation, basé sur un noyau Linux. Partenaire de TiVo, le constructeur Thomson pourrait participer à la commercialisation d'un magnéscope numérique en Europe très prochainement.





## ReplayTV



Le ReplayTV, de Replay Networks, est mis en vente par Panasonic. Plusieurs modèles sont disponibles (ReplayTV 3020 et 3030). Les services Internet du ReplayTV sont, contrairement aux modèles de TiVo, totalement gratuits. Tout comme eux, le ReplayTV se présente sous la forme d'un boîtier et de sa télécommande, que l'on connecte directement au

téléviseur. Le magnétoscope se charge de rapatrier via Internet les programmes de télévision pour la semaine en cours. En tapotant sur quelques touches de la télécommande, l'utilisateur choisit les émissions qu'il souhaite enregistrer. Un disque standard permet ainsi d'enregistrer jusqu'à vingt heures d'émission.

## Quand la PTV fait trembler les chaînes traditionnelles

Face à l'arrivée de TiVo et Replay Network et la commercialisation des premiers appareils aux USA, les chaînes américaines ont réagi curieusement.

Diffuseurs de programmes, elles ont été séduites pas la puissance de cette technologie, n'y voyant au premier abord qu'un super magnétoscope sur lequel on aurait remplacé les cassettes VHS par un gros disque dur. De fait, elles sont vite entrées dans le capital de l'une voire des deux sociétés simultanément (c'est le cas de NBC, Disney et Liberty Media notamment). Mais voilà, de façon contradictoire, ces mêmes chaînes

D'autant plus que cette nouvelle façon de regarder la télévision pourrait grignoter leurs parts de marché en terme de publicité. En effet, il est aisé et peu coûteux pour les deux "start up" de revendre de la publicité très ciblée en utilisant les programmes des chaînes. Une crainte certaine pour les canaux traditionnels si l'on en croit l'étude du cabinet Forrester Research qui estime que le marché de la publicité sur mesure pourrait atteindre les 18 milliards de francs d'ici à 2004.

**"... remplacé les cassettes VHS par un gros disque dur."**

Face à l'engouement des investisseurs (Time Warner ou AOL par exemple, et des construc-

teurs comme Philips ou Sony) pour ces deux sociétés, elles se considèrent en position de force et excluent tout reversement de droits aux chaînes traditionnelles. En outre, elles soulignent qu'elles ne sont pas responsables de la recompilation des programmes, vu que c'est la machine elle seule qui réalise cette tâche.

### Pour en savoir plus...

Les constructeurs de PTV  
[www.philips.com](http://www.philips.com)  
[www.sony.com](http://www.sony.com)

Les fournisseurs  
[www.tivo.com](http://www.tivo.com)  
[www.replaytv.com](http://www.replaytv.com)

overview demo buy now contact us customer care news/events advertise company

1 What is ReplayTV?  
 2 See a Demo  
 3 Get One Now

replaytv

latest news  
 ReplayTV Discs

Win a free ReplayTV!

ReplayTV Special Offers

Some televisions have all the fun.

<http://www.replay.com>



News, dossiers, sélections de sites Web, Logiciels, charme, Fiches pratiques...

Découvrez tout Internet en 132 pages pour 10 F seulement

# Au Scour, la justice s'en mêle

Après Napster, la société californienne Scour et son logiciel d'échange de fichiers multimédias est à son tour sous le feu de la justice américaine. Ces procès posent le problème du respect des droits d'auteurs sur Internet. De son côté, Scour se défend en affirmant ne pas être responsable du contenu passant par ses serveurs.

## Le cousin de Napster



Vaste monde d'échanges libertaire, Internet est souvent considéré comme une zone de non-droit. Les technologies de partage et d'échange de données entre internautes (baptisées peer-to-peer) s'y développent avec fulgurance et avec elles, désormais, les procès contre leurs auteurs. Parce que les fichiers échangés sont pour la plupart des fichiers multimédias - musique au format MP3 ou vidéo au format AVI -, soumis le plus souvent au principe des droits d'auteurs. La bataille pour leur respect apparaît aujourd'hui comme l'un des enjeux majeurs de l'ère Internet. Ainsi en ont décidé les principales maisons de disques mondiales.

Après Napster et ses problèmes avec le groupe Metallica, le rappeur Dr Dre ou la toute puissante RIAA (Recording Industry Association of America), c'est au tour de la société Scour d'être placée rang des accusés à cause de son logiciel Scour Exchange. Et cette fois, les maisons de disques sont soutenues par les grandes majors hollywoodiennes, regroupées au sein de la MPAA (Motion Picture Association of America). Cette dernière n'en est d'ailleurs pas à son coup d'essai, puisque elle tente déjà un procès au magazine américain 2600 Magazine, coupable à ses yeux d'avoir favorisé la diffusion d'un système de décryptage des protections des disques vidéo baptisé DeCSS.

Basée à Beverly Hills en Californie, Scour a tout d'abord développé un site Web ([www.scour.com](http://www.scour.com)) depuis lequel il est possible de télécharger des fichiers musicaux ou des vidéos repérés à l'aide d'un puissant moteur de recherche. Il s'agit d'un très bon moyen pour découvrir des bandes-annonces de films à venir ou diffuser certains genres (comme des court-métrages) boudés par les circuits traditionnels. En somme, rien de plus banal dans le monde d'Internet.

Mais Scour a aussi créé un logiciel semblable à celui de Napster, avec lequel, via les serveurs de la société, il est possible de s'échanger toutes sortes de fichiers, dont parfois des films entiers. Pourtant, Scour avait eu une approche plus "légaliste" que Napster puisque des accords avaient été ou étaient en passe d'être conclus avec de grandes maisons de disque et d'édition vidéo comme Miramax, Sony ou AOL-Time Warner. De plus, le principal actionnaire de Scour, Michael Ovitz, est un impresario très connu d'Hollywood. Steven Spielberg, Madonna ou bien encore Tom Cruise ont déjà fait appel à ses services. Il est à ce titre un vieil ami de Jack Valenti, président de la MPAA. Du coup, la plainte déposée par cette association en a surpris plus d'un.

Pour les plaignants, le logiciel Scour Exchange n'est ni plus ni moins qu'un très bon moyen de voler et d'échanger des films sur Internet. Il en résulte donc des dommages financiers et un manque à

gagner pour les maisons de disques. Les exploitants de cinémas y vont aussi de leurs griefs, puisqu'il est effectivement possible de découvrir des films entiers (ce fut le cas avec *Gladiator* ou *Perfect Storm*) avant la fin de leur diffusion dans les salles obscures. Dans ce cas, Internet fait tout simplement très peur, mais n'est pas entièrement à l'origine du problème. Il agit comme un amplificateur d'un phénomène ancien, le piratage et la revente de copies interdites, largement répandu dans les rues.

Le logiciel Scour Exchange est aussi accusé d'être vulnérable et de permettre l'accès à tout le disque dur des personnes l'ayant installé sur leur ordinateur et non pas aux simples fichiers partagés comme prévu. La MPAA demande donc, comme ce qui a failli être obtenu dans le procès Napster, l'arrêt pur et simple du fonctionnement du site et des serveurs de Scour. Ceci aurait pour effet immédiat de rendre inopérant Scour Exchange, qui a besoin de ces serveurs pour fonctionner. En cas de poursuite de l'activité, Scour s'expose à une amende très forte (150000\$ US) pour chaque contenu piraté.

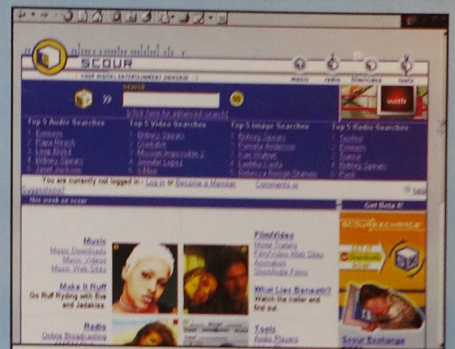
La société californienne a décidé d'adopter une ligne de défense forte, en se basant sur le cas des fournisseurs d'accès à Internet. Ces derniers ont été "dédouanés" de ce genre d'accusation (malgré tout les fichiers échangés par leur seul intermé-

## Scour Exchange mode d'emploi

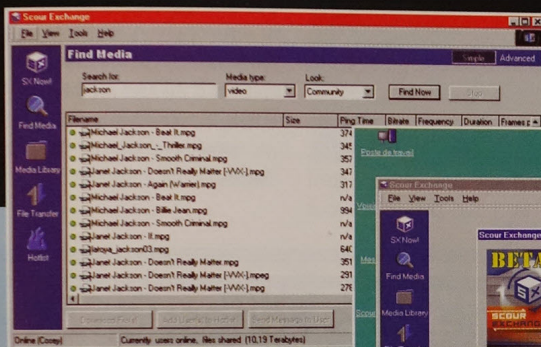
Le logiciel Scour Exchange, téléchargeable depuis le site Scour.com, ne pèse que 1,5 Mo. Il s'installe très facilement sur un PC et son fonctionnement est d'une simplicité enfantine. Après s'être créé un "compte" (il est possible de donner de faux renseignements) et avoir spécifié quel répertoire il souhaitait partager, l'utilisateur peut commencer à rechercher les fichiers de son choix en espérant que d'autres adeptes du logiciel les possèdent. Il dispose pour cela d'une interface simple et claire. Après avoir spécifié le nom de

l'artiste, de la chanson ou du film souhaité, il suffit de cliquer sur le bouton "Find now" pour lancer la recherche. Les critères peuvent être affinés en précisant par exemple type de fichier recherché (audio, vidéo, etc.). Scour Exchange indique alors quelles occurrences il a trouvées. Il suffit alors d'effectuer un double clic sur le ou les fichiers voulus pour lancer le téléchargement.

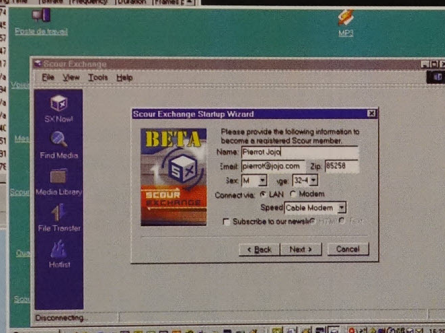
Si votre vis-à-vis et vous-même possédez une bonne liaison, vous pourrez très rapidement profiter de vos nouveaux fichiers.



Au départ, Scour s'est contenté de développer un site Web sur lequel il était possible de télécharger de la musique au format MP3 et des fichiers vidéo. Très bien réalisé, le site comporte un moteur de recherche facilitant la tâche des internautes.



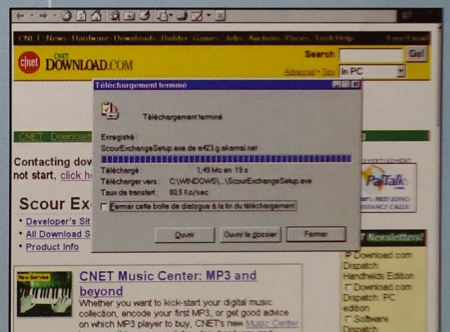
Une interface du même type que celle de Napster.



**Nom:** SCOUR

**Fonction:** échange de fichiers

**Coût:** gratuit



diaire) au motif qu'en tant que prestataire de services, ils ne peuvent être tenus pour responsables des contenus qui transitent par leurs tuyaux. Ce raisonnement apparaît d'une logique implacable. En effet, on ne condamne jamais les sociétés d'auto-roues pour les tonnes de drogues ou de marchandises volées qui transitent par leurs réseaux. Scour considère donc être dans ce cas, se dégageant de toute responsabilité. Et à l'instar des contre-attaques de Napster, elle accuse même les majors de ne pas respecter la loi antitrust et d'être en situation d'abus de position dominante. Condamner l'existence du logiciel reviendrait en effet à empêcher le développement de nouveaux circuits de distribution, ce qui s'apparenterait à des pratiques anticoncurrentielles. Nombre d'artistes indépendants et méconnus n'auraient ainsi aucune chance de connaître un jour la gloire si on empêche la diffusion de leurs œuvres.

Quel qu'il soit, le jugement est très attendu, puisqu'il fera office de jurisprudence dans la bataille des droits d'au-

teurs sur Internet. De plus, en cas de victoire de la NPAA, ce sont les internautes eux-même, individuellement, qui pourraient devenir la cible des plaignants. Cette bataille serait alors loin d'être gagnée mais est envisageable, surtout à l'échelle américaine. De plus, il faut savoir que l'interdiction de logiciels comme Scour Exchange ou Napster ne résoudrait pratiquement pas le problème. Il est très facile d'échanger n'importe quel fichier par l'intermédiaire d'un système de FTP (File transfert protocol) ou même via IRC (Internet relay chat). Et des logiciels spécialisés comme Gnutella ne font appel à aucun serveur pour fonctionner. Dans ce cas, une simple connexion à Internet suffit pour télécharger des fichiers de toutes sortes. Rien de semble donc pouvoir freiner la prolifération des techniques de peer-to-peer, sinon mettre fin à toutes sortes d'échanges sur le Réseau. Mais il est impossible d'interdire Internet !

Pierre Chauveau

Scour Exchange, le logiciel incriminé par les majors hollywoodiennes, se télécharge en quelques minutes depuis le site Scour.com. Il est même disponible sur le très populaire centre de téléchargement de l'américain CNET.

Entre le moment où nous rédigeons cet article et sa mise en place, la société SCOUR décidait la mise en suspend pure et simple de son activité de téléchargement face aux innombrables pressions et menaces qu'elle subissait. Il faut bien souligner que contrairement à Napster, Scour permettait non seulement l'échange de fichiers MP3 mais aussi de fichiers vidéo. Une menace prise très au sérieux par l'industrie du 7e art... Scour se trouvait donc attaqué tant par les professionnels de la musique que du cinéma, une situation intenable qui lui aura été fatale !

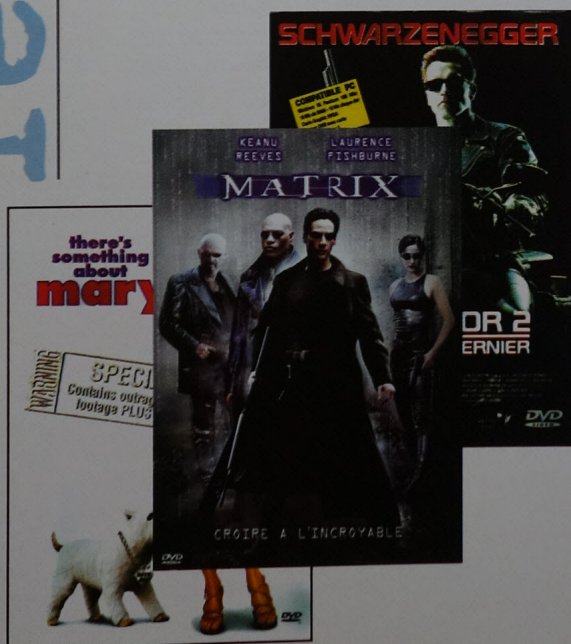
# LE DEZONAGE DES DVD !

Technologie

Les DVD sont protégés ! Pour éviter aux pays Européens de souffrir de la concurrence des américains moins taxés sur les supports vidéo, les majors du Home Vidéo (Fox, Warner et consorts) avaient prévu de séparer le globe en différentes zones... Quatre ans après l'arrivée du DVD sur le marché, on en rigole encore...

Lorsque le DVD a commencé à apparaître sur le marché, que seuls deux ou trois films constituaient la vidéothèque disponible, les grands de l'édition de supports vidéo faisaient trembler les utilisateurs : Non, les lecteurs DVD ne sauraient lire qu'une seule zone, il en serait ainsi et pas autrement... L'objectif avoué de ces grandes industries, c'était bien de cloisonner les marchés à l'ère de la globalisation économique...

Certes, mais aujourd'hui, la répartition en zones géographiques n'est plus qu'une vaste plaisanterie dont se raillent tant les utilisateurs que les producteurs de lecteurs, qu'il s'agisse de lecteurs de salon (sous forme de platines) ou de lecteurs de DVD-Rom (installés sur Mac ou PC). Le dézoning est devenu une pratique habituelle, qui n'effraie plus personne et n'émeut même plus les éditeurs eux-mêmes qui ont un peu honte d'avoir cherché à nous imposer leur Diktat commercial.



## La répartition en zones

Contrairement à une idée trop répandue, le monde du DVD n'est pas divisé en six zones mais en huit. En effet, les deux zones méconnues sont réservées à des usages spécifiques puisque la septième zone est encore en suspens, conservée en réserve, alors que la zone numéro huit est, quant à elle dédiée aux avions de ligne. Un statut spécial qui est dû au fait qu'en vol, les avions obéissent à des législations particulières...

La zone qui, en terme de catalogue offre le plus d'intérêt, c'est bien évidemment la zone qui correspond à l'Amérique du nord : La zone 1. Avec un catalogue de plusieurs milliers de titres, depuis les dernières nouveautés qui sortent alors qu'elles sont encore en salle en France, jusqu'aux grands classiques, des trésors pour cinéphiles sont disponibles. Et pour peu que vous

commandiez sur Internet, vos DVD, ne vous coûtent plus que 100 à 150 Francs contre 250 Francs en import à la FNAC... Une réalité qui fait réfléchir, non ?

L'Europe et l'Asie se partagent quant à elles, la zone 2. Aujourd'hui le catalogue tend à être de plus en plus fourni, même s'il faut reprocher la piètre qualité des bandes son en Français. En effet, alors que les versions originales sont souvent en Dolby Digital 5.1, nous devons nous contenter d'un vague Dolby Surround 2.0 qui laissera pantois les puristes... Les pays d'Asie du Sud Est (Indonésie etc.) se partagent la zone 3, la zone 4 vaut pour l'Amérique du sud et l'Australie. La cinquième zone est réservée à l'Afrique et à la Russie, et enfin, la sixième zone (c'est presque un titre de film), s'applique à la Chine...

## Une zone, des zones: dézone...

Allez trêve de plaisanterie, tout le monde sait très bien qu'il n'y a rien de plus simple que de dézoner un lecteur de DVD. Selon votre configuration, plusieurs modes existent. Pour les lecteurs de salon, deux postulats sont possibles : Le premier consiste à un dézoning logiciel. Effectuez une combinaison de touches sur la télécommande ou sur le lecteur lui-même et (Ô Miracle !) votre lecteur devient compatible avec toutes les zones.

Ca c'est dans le meilleur des cas, car pour certains modèles, il faut en venir à une manipulation électronique en coupant la patte d'une puce en général.

Une configuration plus ennuyeuse car toute modification portée à la machine implique la perte de la garantie.

Soyez donc sûr de votre coup car vous pourriez bien le regretter en cas d'erreur...

Pour les lecteurs de DVD-Rom, le

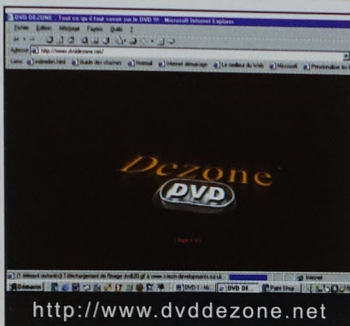
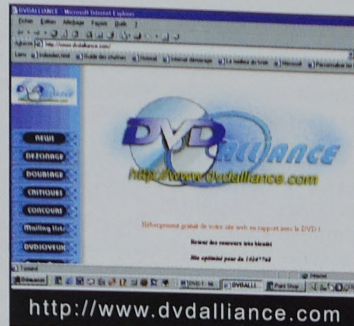
dézoning peut s'appliquer à plusieurs niveaux. En effet, si le lecteur peut physiquement être dézonné grâce à un patch que vous pouvez télécharger sur le Net, il faudra bien souvent agir également sur la carte de décompression Mpeg-2 qui vous permet d'afficher le contenu du DVD, ou encore sur votre carte d'affichage.

Mieux encore, il arrive parfois pour les lecteurs de DVD-Rom que l'interface qui leur est dédié vous propose un certain nombre de changements de zone limité. Nul besoin de vous dire que ce genre de petites protections, il n'y a rien de plus simple à faire sauter... Une fois encore de nombreux patch, ou de nombreux "pas à pas" que vous trouverez sur le Net, vous guideront dans toutes les étapes du dézoning de votre lecteur.

## Mettre le Net à profit

Il existe aujourd'hui pléthore de sites sur le Web qui se font fort de vous donner tous les renseignements nécessaires au dézoning de votre lecteur. Interdite bien sûr, mais vaguement tolérée, cette pratique vous ouvrira alors les catalogues de tous les éditeurs dans le monde entier.

Deux sites ont particulièrement retenu notre attention et si vous comptez franchir le cap des zones géographiques. Nul doute en effet que le modèle de lecteur qui vous équipe figurera dans leurs bases de données car ces sites sont de véritables cavernes d'Ali Baba. N'hésitez donc pas à pointer votre navigateur sur [www.dvdalliance.com](http://www.dvdalliance.com) ou encore sur [www.dvddezone.net/progs.html](http://www.dvddezone.net/progs.html) qui vous fournit une grande quantité de liens vers de petits patches qui feront votre bonheur, c'est certain...



## Le Div-X : Mp3 du cinéma

Le Mpeg4 est un nouveau format de compression dans la lignée du mp3 pour l'audio, l'algorithme Mpeg4 divise la taille des fichiers Mpeg-1 par 3. Ceci permet d'obtenir, au choix, une qualité supérieure, ou un temps de stockage multiplié par 3. Cette véritable révolution est apparue sur le Net en janvier 2000.

Depuis, ce sont près de 1000 films qui ont été ainsi distribués, avec une qualité parfois contestable mais qui ne cesse de progresser. Pour que votre ordinateur puisse interpréter correctement un film au format mpeg4 il faut disposer, sur votre machine, des drivers Divx que vous trouverez eux aussi sur le réseau...

## DeCcss: La fin d'un espoir ?

Les studios de cinéma hollywoodiens (Universal, filiale de Seagram Co. Ltd., Metro-Goldwyn-Mayer Inc. et Time Warner) espèrent remporter d'ici une semaine une victoire décisive dans leur offensive judiciaire contre le piratage des films sur internet.

En début d'année le journaliste Eric Corley est devenu le cauchemar des majors du cinéma car il a dévoilé l'existence d'un fantastique utilitaire appelé Decode Content Scrambling System (DeCcss).

Pour la MPAA (Motion Picture Association of America), la situation est inacceptable car l'unique objet du DeCcss est de pirater les DVD (Un point de vue comme un autre !).

Ce procès n'est pourtant qu'un aspect de la lutte que livre l'industrie du spectacle pour protéger ses intérêts sur le Net. En effet, rappelons que, de son côté, la RIAA (Recording Industry Association of America), cousin de la MPAA, mène une guerre identique contre Napster...

## Dézoning : Légal, pas légal ?

Pour trancher sur la question, le mieux était encore de s'adresser à un homme de loi. Pascal Alix a accepté de répondre à nos différentes interrogations. Avocat, il est également le webmaster du site [www.virtualegis.com](http://www.virtualegis.com)...



1. Est-il permis d'acheter des DVD d'une autre zone que celle qui nous concerne via Internet ?

PA : L'acquisition n'est pas critiquable en soi, dès lors que le DVD est, au sens juridique "dans le commerce" (sur le Net notamment). Aucun délit ne peut être présumé à ce stade.

2. Peut-on sans problème procéder au dézoning d'un lecteur DVD ?

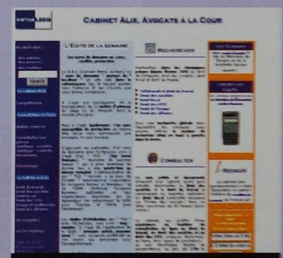
PA : Pour l'instant, la loi française est muette. Les associations de défense des producteurs parlent de "piratage", mais sans qualifier juridiquement. En l'absence de texte précis, je ne vois pas là une contrefaçon, ni un autre délit, chacun étant libre de modifier le matériel qu'il acquiert (le droit à la modification du bien fait partie du droit de propriété). Mais il est clair que le dézoning est parfois un moyen de lire des disques contrefaisants, notamment en provenance d'Asie du sud-est. Dans ce cas, il peut y avoir recel du délit de contrefaçon.

3. Dans le cas contraire, quelles sont les peines qui peuvent être encourues ?

PA : Si l'on s'en tient au dézoning (assez facile) du lecteur DVD, aucun délit ne semble prévu par le code pénal français.

**"... il peut y avoir recel du délit de contrefaçon."**

Si le dézoning est le moyen d'accomplir un acte de contrefaçon ou de procéder sciemment à la lecture d'un disque contrefaisant, les peines de la contrefaçon sont applicables. Sachant toutefois que le consommateur final est rarement poursuivi sur le plan pénal.



[www.virtualegis.com](http://www.virtualegis.com)



Outlook, Access, Power Point, mais aussi Internet Explorer : toutes ces applications ont connu des problèmes plus ou moins graves liés à la sécurité. Les logiciels de Microsoft sont-ils de vraies passoires?

Les événements se succèdent et se ressemblent : chaque sortie d'un produit Microsoft est systématiquement suivie de celle d'un Service Pack, c'est à dire un patch correctif. Actuellement Microsoft doit encore faire face à une sérieuse faille de sécurité récemment découverte dans ses logiciels de messagerie Outlook et Outlook Express. A cause de ce bug de sécurité, un pirate serait capable de prendre le contrôle d'un PC à distance simplement en envoyant un e-mail. Il pourrait en effet profiter d'un bug d'Outlook lié à un dépassement de la mémoire tampon et qui évacue le surplus de caractères du champ " date " dans la mémoire vive. Une fois que ces informations sont stockées dans la mémoire, elles peuvent donc être exécutées, et provoquer toutes sortes de dégâts (effacement de certains fichiers, prise de contrôle du PC à distance, etc.) Les versions d'Outlook Express concernées par cette faille sont les 4.0 et 4.01. Quant à Outlook, il s'agit des versions 98 et 2000. Microsoft a immédiatement réagi et propose depuis le 19 juillet plusieurs solutions : télécharger Internet Explorer 5.01 Service Pack1 ou la version 5.5 d'Outlook Express, comprise dans ce même navigateur (sauf pour Windows 2000). Pour ceux qui ne veulent pas télécharger des mégas de données ou qui utilisent Outlook, un patch est disponible à l'adresse suivante :

[www.microsoft.com/windows/ie/download/critical/patch9.htm](http://www.microsoft.com/windows/ie/download/critical/patch9.htm)

## Internet Explorer encore vulnérable

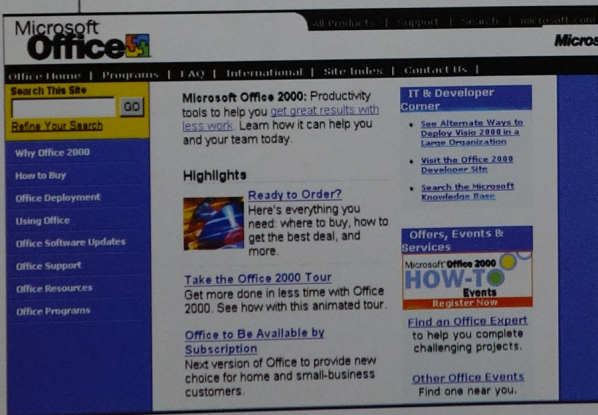
Comme si cela ne suffisait pas, le tout nouveau navigateur de Microsoft, Internet Explorer 5.5, connaît lui aussi des soucis liés à la sécurité. Il semble que cela concerne aussi les navigateurs 4.X, 5.0 et 5.01. Un contrôle Active X défaillant permet dans certaines conditions à un administrateur de sites Web d'accéder à vos fichiers et d'y effectuer des modifications. Un attaquant peut créer un faux fichier d'aide et le placer dans un emplacement accessible par la victime. Il peut créer un fichier compilé d'aide HTML qui sera ouvert par un script sous Internet Explorer. Des fichiers d'aide peuvent également être ouverts dans d'autres environnements qui supportent le " scripting " actif, tel que des e-mails sous Outlook. La réaction de Microsoft -encore une fois-, a consisté à proposer des mises à jour de ses produits. Mais il n'y a pas de correctif disponible pour la version 5.5 d'Internet Explorer. Est-ce dû à une lenteur des développeurs du géant de Redmond ? Selon un article disponible sur Internet, il semblerait plutôt que cette version d'Explorer soit aussi concernée par ces soucis de sécurité. Nous attendons donc, une fois de plus, un correctif de Microsoft.

Ce n'est pas la première fois que Internet Explorer a des soucis de sécurité. Il en a d'ailleurs connu dès sa sortie. Baptisé " cross-frame navigate issue " (problème de navigation inter-plate-forme), ce bogue concernait tout autant les versions Windows et Macintosh d'IE 3.x et 4.x. IE contenait à l'origine une commande ActiveX située dans le module d'édition de scripts DHTML Edit Control. Il y a problème si le webmaster utilise la commande IFRAME avec cet éditeur. Le HTML dynamique de Microsoft (DHTML) édite en effet à ce moment un composant autorisant un administrateur ou à des créateurs d'applications d'avoir un contrôle depuis leurs sites sur des fichiers situés sur des ordinateurs distants. En bref, n'importe qui se connectant à votre site Web pouvait accéder à l'arborescence du disque dur hébergeant ce site.

Mais les soucis de sécurité ne sont pas le simple apanage des applications directement liées à

Internet. La gamme Office est elle aussi concernée par des problèmes de sécurité. Il existe en effet de nombreux virus Macro qui utilisent les fonctions d'exécution automatique de nombreux logiciels de cette suite bureautique pour se développer. Excel 2000, Power Point 2000, Access 2000, Word 2000, Photodraw 2000, Frontpage 2000, Project 2000, Publisher 2000 et Works Suite 2000 -rien que ça !- sont concernés. Autre problème, il existe une commande ActiveX qui se présente comme un élément d'Office 2000 et qui est désigné, bien par erreur, en tant que " safe for scripting " (sécurité d'écriture). Baptisée Office 2000 U. C., cette commande sert à la fonction "Qu'est ce que c'est?" des rubriques d'aide. Elle est destinée en fait à contrôler par script certaines fonctions d'Office. Un opérateur de site Web, avec de mauvaises intentions, pourrait employer cette commande afin d'exécuter des fonctions d'Office sur la machine d'un utilisateur qui a visité son site. Il pourrait s'agir de fonctions aux conséquences nulles comme de fonctions d'effacement ou de formatage de disque. Un patch pour empêcher cela est disponible à l'adresse suivante : <http://officeupdate.microsoft.com/info/ocx.htm>

La dernière mise à jour disponible sur le site de Microsoft concerne Windows 2000. Il s'agit du Service Pack 1. Fort de ses 83 Mo (!), il se propose de corriger des bugs de sécurité et d'améliorer la stabilité du système d'exploitation - encore une fois -. La liste de ces bugs, impressionnante, est disponible sur Internet. Ces correctifs s'appliquent aux versions Professional, Server et Advanced Server de Windows 2000. Ce service Pack sera intégré aux prochaines versions de Windows. Mais qu'advient-il des utilisateurs qui ne la posséderont pas et qui devront se retrouver avec une pléiade de CD de Service Pack à installer après un formatage et une restauration du système ? Car il est certain qu'après le Service Pack 1, il en viendra un second ! Voici l'adresse à laquelle vous pouvez télécharger le Service Pack 1 : [www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp](http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp)



le site de Microsoft Office

# D'UN BUG ANNONCE !

## Les virus savent utiliser la moindre faille d'un système

Mais quelles sont les conséquences de ce manque de sécurité dans les produits Microsoft ? Le dernier exemple que tout le monde a encore en tête est celui du virus ILOVEYOU qui a su tirer parti des failles dans le système de sécurité d'une des applications de Microsoft Office. Ce Virus a été écrit en langage Visual Basic. Il se présente sous la forme d'un fichier attaché au mail avec une extension .VBS cachée. Il apparaît sous la forme ILOVEYOU.DOC (ou \*\*\*\*\*.DOC), mais si dans les options d'affichage vous décochez l'option "masquer les extensions dont le type est connu", vous verrez l'extension .VBS apparaître. Il se présente généralement sous la forme de courrier transféré. En lançant le fichier attaché, le virus va d'abord modifier les deux clefs suivantes du registre de Windows: HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run et HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices. Il va ensuite se copier sur le disque dur en prenant le nom d'un des fichiers existants dans le répertoire C:\windows\recent. Enfin, il va se propager en utilisant le carnet d'adresses d'Outlook et s'auto-envoyer aux adresses qui y sont notées. Enfin, dernier petit détail, il va modifier les extensions des fichiers images .JPEG et musicaux .MP3 en .VBS. La faille au niveau de la sécurité d'Outlook a permis une propagation très importante du virus, en lui permettant un accès à sa base de données et en lui laissant le champ libre pour l'envoi de messages à l'insu de l'utilisateur de la messagerie. Ce fonctionnement n'est pas sans rappeler un autre virus, Melissa, apparu en mars 1999. Le CERT (Computer Emergency Response Team) avait annoncé à l'époque la propagation d'un nouveau genre de virus qui se diffusait par courrier électronique. Melissa appartient

à la famille des virus Macro qui font partie intégrante des documents du traitement de texte Microsoft Word. Ce virus s'attaque au modèle "normal.dot" utilisé lors de la création de tout nouveau document Word. Le simple fait de lire un fichier Word ou de le transmettre permettait la propagation du virus. Enfin, Melissa utilisait les 50 premières entrées des carnets d'adresses électronique au format Mapi. Si le logiciel Outlook était installé sur la machine infectée, il expédiait automatiquement un fichier Word aux 50 futures victimes.

Un Email infecté par Melissa avait pour sujet la phrase " Important message from... ", suivit du nom du correspondant infecté, qu'il avait volé dans le carnet d'adresses. Dans le texte, se trouve un fichier attaché (le fichier Word infecté) et le message " Here is the document that you asked for, dont show anyone else ;-)." Selon le CERT, Melissa ne concernait que les PC équipés de Microsoft Word 97 et Word 2000 et ne se diffusait que par Outlook

Microsoft avait eu un premier avertissement avec ce virus qui a su utiliser les failles d'un système. La firme de Bill Gates n'en a pas tenu compte. Il aura fallu attendre l'apparition d'un autre virus, aux conséquences bien plus graves, pour qu'ils décident, enfin, de travailler sur une solution efficace ! Effectivement, un correctif est sorti et nous pouvons dire qu'il s'attaque au problème viral de façon plutôt radicale. Il bloquera tout simplement les exécutables de type .exe, .reg (qui sert à modifier la base de registre), et .cmd s'ils sont transmis en pièces jointes ! il n'y aura plus la possibilité d'exécuter les pièces jointes, ni de les enregistrer sur le disque dur ! Toutes les intrusions par un programme inconnu dans le carnet d'adresses Outlook sera signalée. Enfin, les paramètres de sécurité seront tous activés de façon à éviter que les scripts

## Outlook encore en cause !

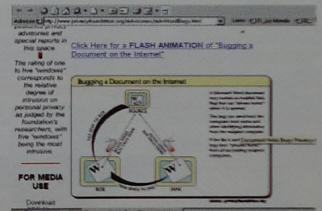
Le manque de fiabilité d'Outlook, le logiciel de messagerie de Microsoft, n'est plus à démontrer. En plus de " faciliter " la propagation de virus via le carnet d'adresses de l'utilisateur, il bloque l'installation de certains logiciels ! Incroyable mais vrai : lorsqu'on installe un logiciel sur son ordinateur et qu'Outlook est ouvert en tâche de fond, l'installation fige à la fin, la jauge

indiquant 99 %, en plus de mettre un temps plus long que la normale. Outlook 2000 est le seul responsable puisqu'il suffit de quitter l'application pour que tout rentre dans l'ordre. Toutefois, nous vous conseillons de le supprimer de votre disque dur et d'utiliser Outlook Express (fourni avec Windows 98) pour éviter ce genre de désagréments !

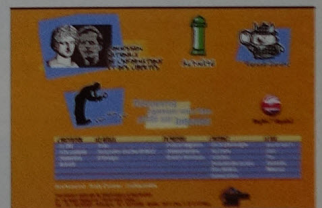
Visual Basic et Javascript, ainsi que les contrôles ActiveX, ne s'exécutent d'eux même. Evidemment cette hausse du niveau de sécurité ne reste pas sans conséquences sur la compatibilité avec d'autres applications dont la liste est disponible sur le site de Microsoft : <http://officeupdate.microsoft.com/2000/downloadDetails/Out2ksec.htm>

À travers ce durcissement, c'est encore une fois le particulier qui paie ! Il se voit limité dans l'utilisation de son programme de messagerie. Cela dit, la personne qui ne souhaite pas installer ces mises à jours est libre de ne pas le faire, mais elle risque d'avoir très vite des soucis. Encore faut-il relativiser les choses. Avec un minimum de précautions, il est tout à fait possible de passer au travers d'attaques de virus : mise à jour hebdomadaire, méfiance envers les attachements inconnus, ou utilisation d'un logiciel de messagerie comme Eudora, non concerné par ces problèmes de sécurité. Les virus qui ont su utiliser les failles de sécurité de Microsoft étaient " gentils." Ils ne s'attaquaient pas au hardware comme le CIH par exemple, appelé aussi

Tchernobyl. Mais il est quand même dommage de devoir procéder à un formatage et une restauration de son système parce que Microsoft fait preuve de trop de négligences au niveau de la sécurité de ses applications. Louis Neveu



les explications de la Privacy Foundation aux US sur les mouchards présents dans les programmes ou les e-mails ([www.privacyfoundation.org](http://www.privacyfoundation.org))



le site de la CNIL qui se penche sur le dossier et ses implications juridiques

# Enchères nazies : YAHOO!® condamné, Internet menacé ?

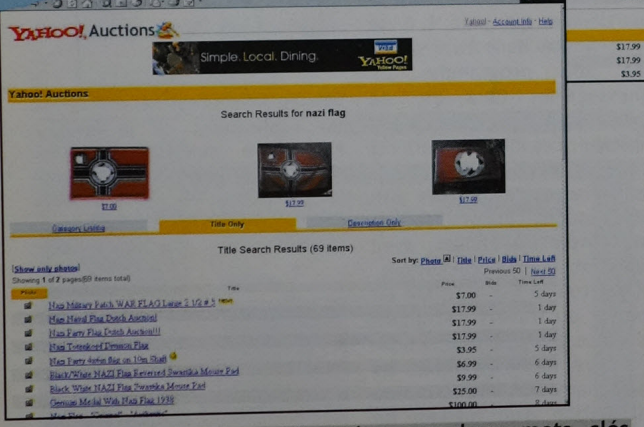
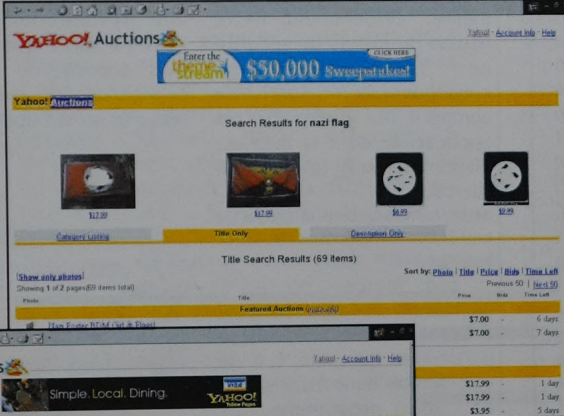
Un tribunal français condamne la société américaine Yahoo ! à interdire l'accès des internautes français à ses pages de vente aux enchères d'objets nazis. En plus de la quasi impossibilité technique de se conformer à un tel jugement, se pose le problème de la législation d'Internet.

## L'affaire Yahoo! Un cas qui devrait faire jurisprudence

Au tout début, Internet était une immense zone virtuelle de liberté sur laquelle aucun contrôle n'était réellement exercé. Puis, petit à petit, ce nouveau média a émergé pour parvenir au succès qu'on lui connaît aujourd'hui. De nombreuses "affaires" sont régulièrement venues ternir l'image de communauté virtuelle, notamment dans le monde des enchères. La première grosse alerte survint lorsqu'un rein fut mis en vente pour un million de francs sur le site français Aucland. Malgré les nombreux efforts des censeurs pour retirer cette annonce du site d'enchères, elle réapparaissait sans cesse, le vendeur changeant continuellement de pseudonyme. Face à cet acte insolite, qui défraya la chronique, et dont on ne saura jamais s'il tenait plus du

canular que d'une vente réelle, les autorités françaises avaient immédiatement convoqué les responsables de sites d'enchères français afin de mieux contrôler le contenu des ventes de particuliers à particuliers. D'où le développement d'une charte, sorte de code de bonne conduite, que les responsables de ces sites appliquent avec plus ou moins de pertinence. Mais en l'absence de textes de lois, clairs et précis, la censure est laissée à leur libre appréciation.

Cette charte interdit de mettre en vente des articles litigieux, contrairement aux lois ou au code civil. Mais rien n'empêche un vendeur malveillant de passer une petite annonce concernant un produit illicite. Les équipes responsables du contrôle du respect de la charte lisent tout ce qui est mis en ligne mais avec un certain délai (l'entrée d'une annonce est automatique et sa publication immédiate). C'est pour cette raison que certaines annonces frauduleuses peuvent rester visibles pendant quelques heures ! Mais le pire est que le vendeur peut très bien jouer sur les mots et rédiger une annonce ambiguë que seuls des initiés comprendront. La plus grande hypocrisie règne donc dans le domaine du respect de cette charte ! Car si les censeurs ont le réflexe de supprimer des annonces concernant des articles de guerre nazis, il se montrent bien plus souples, voire laxistes, avec les annonces concernant la vente de copies de logiciels : les annonces à 10 F le CD remplis de nombreux jeux pour consoles sont monnaies courantes sur iBazar ! En règle générale, les articles taxés de censure sont les alcools, tabacs, stupéfiants, armes de guerre, organes, et tout type de contrefaçon.



Recherches effectuées sur deux mots clés dans différents moteurs de recherche...

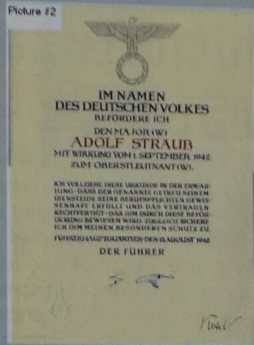
	nazi	Hitler
Google.com	626 000	417 000
Altavista.com	206 890	175 450
Altavista.fr	9410	9185
Lycos.fr	3885	5301
Yahoo.com enchères	1837	387



## Des documents paraphés de la main d'Adolf Hitler

### Vu sur Ebay...

Un illuminé vend pour des sommes colossales, des documents paraphés par Hitler et divers officiers nazis. Yahoo n'est donc pas le seul site à mettre en cause dans la mise en vente d'objets datant de la période nazie.



rendre possible l'accès aux pages d'enchères américaines (qui n'ont d'ailleurs pas besoin de lui pour être vues depuis n'importe quel poste connecté à Internet.) Les internautes de notre pays accèdent ainsi à un contenu jugé frauduleux. " La vente de ces articles constituent une apologie du nazisme ou une contestation des crimes nazis " proclame Jean-Jacques Gomez, juge des référés au tribunal des Grandes Instances de Paris, qui, le 22 mai dernier, a entendu la plainte des deux associations. Il a condamné Yahoo ! Inc. à rechercher des solutions pour interdire l'accès à ces pages depuis le territoire français. A cette occasion, un délai de trois mois a été laissé à la société et sa filiale française pour proposer ses solutions.

Le 25 juillet dernier, toutes les parties se sont retrouvées au tribunal, pour entendre les propositions du site phare de l'Internet. Yahoo ! a mandaté à cet effet une société spécialisée dans la sécurité sur Internet, Edlweb qui tire les conclusions suivantes : "il n'existe pas en l'état actuel des techniques présentées, de mesures pouvant être mises en œuvre sur le site de Yahoo - ou de tout autre site - répondant en tout point à cette demande". Un constat sur lequel s'est appuyé la défense de Yahoo !, son avocat, maître Pecnard, ayant déclaré qu'aucune méthode d'interdiction n'est incontournable, qu'elle soit logicielle, matérielle, ou

humaine. Et l'avocat de la partie adverse de renchérir aussitôt : " si on ne peut pas filtrer, alors qu'on éradique ". Des propos quelque peu radicaux, impossibles à appliquer sur le réseau mondial. Plus grave : faire respecter les lois françaises à une entreprise américaine ne correspond pas à l'esprit des lois en vigueur au plan international. Certes la vente de certains objets sont interdits en France mais doit on faire appliquer la législation française à une société se situe à des milliers de kilomètres de nous pour essayer de rendre Internet compatible avec des lois spécifiques à un pays ?

Yahoo ! Inc ne pense pas être en mesure de mettre en place des solutions techniques pour satisfaire la justice française. De plus, il n'appartient pas à celle-ci de dire à telle ou telle entreprise américaine ce qu'elle doit faire, sauf à imposer des solutions disproportionnées, dans le cas présent, et à lui faire jouer le rôle de "censeur".

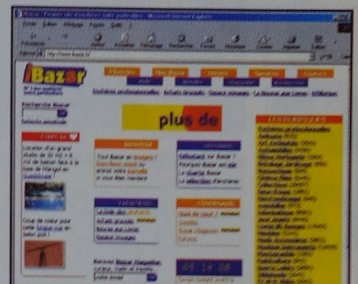
S'il est incontestable que certains objets ne doivent pas figurer sur le Net à cause de leur caractère illicite, il ne faut pas non plus que l'ensemble des lois d'un pays s'impose à l'ensemble du Web. Comment ne pas imaginer un pays interdisant, par exemple, la vente d'un livre tel que celui de Salman Rushdie qui obligerait l'accès à cet ouvrage pour les internautes du pays en question. Cela pourrait vite devenir un casse tête insoluble !

Internet doit rester une zone de liberté, ce qui ne veut pas dire non plus, une zone de non droit... Il est clair que le problème se pose autrement, et une fois de plus, la solution doit passer par une responsabilisation de l'internaute. Se connecter à Internet est un acte volontaire et relève de la liberté individuelle. Nul n'étant censé ignorer la loi, chacun connaît les risques qu'il encourt en se procurant des articles illicites tels que des objets interdits en France. Porter plainte contre Yahoo ! n'arrangera certainement pas les choses. De petits plaisantins vont même sûrement en profiter pour teinter leurs annonces d'un humour très noir. Et quand bien même Yahoo ! trouverait la solution miracle, rien n'empêcherait un collectionneur d'acheter ses articles dans une boutique électronique aux Etats-Unis ou directement auprès d'un particulier.

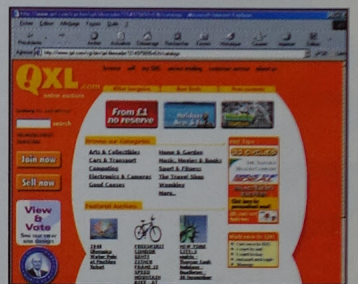
En conclusion, l'affaire Yahoo ! ouvre ainsi pour la première fois le vrai problème de la législation sur Internet, et plus globalement induit une notion de législation mondiale. Et cela montre la faiblesse de notre système face à l'essor de la nouvelle économie. Appartient t'il à Yahoo ! d'interdire à son public de consulter ce qu'il est venu chercher ou à l'Etat français de créer un organisme chargé de contrôler tous les contenus illicites qui pourraient atteindre nos disques durs ? Ce genre d'organisme - dont Lionel Jospin a promis la création prochaine- aurait une fonction équivalente au CSA, à savoir contrôler, censurer et faire payer des amendes aux contrevenants. Toutefois, les moyens qui seraient mis en œuvre pour contrôler les citoyens français "circulant" sur le Web seraient contraire aux lois informatique et libertés. La solution du problème s'annonce donc forcément complexe.

Le problème reste donc entier même après la condamnation récente de Yahoo! à empêcher l'accès aux objets incriminés. Deux sphères d'intérêts s'opposent donc fondamentalement, d'une part la loi française très restrictive et d'autre part ce fameux libéralisme à tout va qui caractérise si bien nos amis américains. Quoiqu'il en soit la décision du 20 novembre obligeant Yahoo! US à filtrer les internautes français aura l'effet d'un tremblement de terre au niveau planétaire. C'est la première décision de ce type. Un évènement qui ouvre le champ à une possible régulation d'Internet.

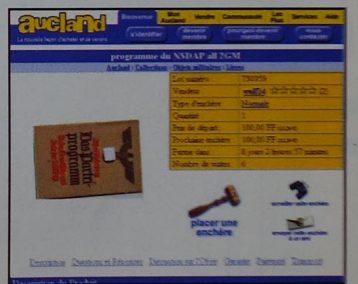
A suivre donc...



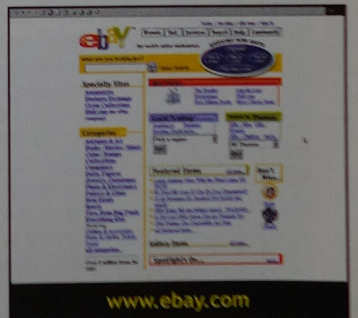
Le leader des sites d'enchères français a plutôt bonne réputation, on peut juste lui reprocher d'être parfois un lieu de vente pour objets pas chers, " tombés du camion " !  
[www.ibazar.fr](http://www.ibazar.fr)



QXL est l'un des concurrents directs de iBazar. Moins connu, on y trouvait tout de même, juste avant l'affaire Yahoo, des objets nazis.  
[www.qxl.fr](http://www.qxl.fr)



En vente sur Aucland, site d'enchères français, un manuel de propagande allemand émanant du NSDAP, parti qui a permis à Hitler d'accéder au pouvoir en Allemagne.





## Enchères nazies : Yahoo condamné, Internet menacé ?

### L'anonymat permet tous les excès !

Les sites d'enchères sont rapidement devenus d'excellents moyens de vendre et d'acheter des objets de toutes sortes. Leur succès est tel que des sites portails se sont mis à proposer à leur tour ce genre de services. Ainsi Yahoo !, Lycos, Wanadoo, pour ne citer que les plus connus, possèdent une section Enchères. Il faut dire qu'en matière de vente de particuliers à particuliers, ce nouveau genre de commerce en ligne n'offre que des avantages. Si le site ne se charge uniquement que de mettre en relation vendeurs et acheteurs, la convivialité qu'apporte Internet fait le reste. Le vendeur passe ainsi une annonce qui peut être lue potentiellement dans le monde entier ; intéresser plusieurs individus qui devront alors "se battre" pour remporter la vente ; et chacun peut intervenir par l'entremise d'une rubrique courrier. Autre atout : la disparité de ces sites qui proposent toutes les catégories d'objets. On peut aussi bien vendre des vignettes Pokemon qu'une automobile de prestige ! Enfin, les transactions sont anonymes puisque chaque intervenant doit d'abord s'inscrire sur le site en déposant ses identifiants : un pseudonyme et un mot de passe. Le pseudo permet au vendeur de cacher son identité, mais aussi de vendre des objets plus ou moins délictueux.

Certains magasins qui ont pignon sur rue, n'hésitent pas à vendre via ce biais, donc sans déclarer leurs ventes. D'autres revendent des articles interdits par la loi, comme des organes (un cas relevé chez Aucland), ou des objets de l'ère nazie. Nous ne pourrions limiter les sites d'enchères uniquement à cela car ceux-ci constituent un excellent moyen de trouver ce que l'on ne possède pas, à des prix souvent intéressants et, plus surprenant malgré l'utilisation de l'informatique, avec une certaine humanité dans les rapports. Qui sait ? Peut-être rencontrerez-vous votre prochain(e) ami(e) sur Ibazar !

### Question à...

**Marc Knobel** *Centre S. Wiesenthal*

Que répondez-vous à ceux qui sont pour la liberté totale sur le Web ?

C'est de la folie ! Même si Internet est un village planétaire, il faut bien nuancer et ne pas tout mettre sur le même plan. Il convient de voir d'où provient l'internaute; dans le cas d'un français, il est soumis aux lois de la République...

La liberté d'expression est une notion fondamentale mais lorsque les 148 pays se sont réunis en 1948 pour définir la Déclaration universelle des droits de l'Homme, il a été convenu que "...ne peuvent être autorisés un état de guerre..." (notamment vis à vis d'un peuple) et que "...l'on ne peut pas aller jusqu'à la haine raciale...". Alors je vous le demande, comment autoriser les sites appelant au meurtre ou à la haine sans transgresser ces notions de base!

### Des solutions techniques très aléatoires

Depuis que Yahoo ! et sa filiale française ont été obligés de proposer et mettre en œuvre des solutions pour empêcher aux internautes français l'accès à la partie du site d'enchères de Yahoo.com où sont mis en vente des objets nazis, de nombreuses questions se posent quant à la faisabilité technique d'une telle requête. Jerry Yang, PDG et fondateur de Yahoo ! l'a même qualifiée de "naïve". En effet, la structure même d'Internet, où les données circulent à travers de nombreux serveurs de pays en pays, rend pratiquement impossible le contrôle de la nationalité des visiteurs par un site. C'est à se demander si les avocats de la Licra et de l'UEJF, ainsi que le juge qui a rendu ce jugement, pourront faire appliquer la décision de justice.

Cependant, les progrès technologiques, venus notamment du monde commercial (où ils servent à mieux connaître les acheteurs), permettent d'envisager la mise en œuvre de solutions de reconnaissance du visiteur. Deux familles se distinguent. L'une où le contrôle se fait depuis le poste de l'internaute et l'autre où il a lieu chez l'hébergeur des pages éventuellement interdites.

La première famille de solutions demande la collaboration de l'éditeur de contenu, de l'internaute et son FAI. Comme pour les sites pornographiques interdits aux mineurs, il faudrait que Yahoo ! "classe" les pages proposant des objets nazis aux enchères dans une catégorie précise, à l'aide de l'insertion d'un identifiant dans le code HTML de ces pages. Cet identifiant serait détecté par un logiciel de filtrage qui interdirait alors l'affichage des pages depuis le poste sur lequel il serait installé. De nombreux programmes de ce type existent déjà, comme Norton Security System 2000 de l'éditeur Symantec. Celui-ci dispose d'un module de contrôle parental interdisant l'accès à certaines pages repérées par des mots-clés. Cette solu-

tion est donc techniquement faisable, mais elle ne l'est pas d'un point de vue conceptuel. Il faudrait en effet installer le logiciel adéquat sur tous les postes reliés à Internet susceptibles d'être utilisés par des français, ce qui représente un travail presque incalculable. Si cela est envisageable sur des postes "publics" (ceux des universités par exemple), comment le rendre obligatoire chez les particuliers sans prendre, par ailleurs le risque de voir se développer des plug-ins (ajouts logiciels) permettant de contourner ces limitations ?

La seconde réponse à ce problème serait mise en place sur les serveurs de Yahoo ! Elle consisterait à localiser la provenance géographique du visiteur grâce à certaines données comme la langue de son navigateur et surtout son adresse IP. Cette série de chiffres (du genre 124.124.189.21) identifie individuellement chaque poste connecté à Internet. En l'état actuel des choses, les experts techniques estiment cette solution valable à 80% seulement, ce dont risque de ne pas se contenter la justice. La société Infosplit, basée à New York mais fondée par des français, a immédiatement réagi à ce problème, affirmant disposer d'une solution dont l'efficacité se situerait entre 95% et 100%. Son fondateur, Cyril Hourri, fut d'ailleurs appelé à la barre durant le procès pour faire la démonstration des qualités de ce logiciel. Grâce à ses puissants algorithmes, il est censé pouvoir localiser le pays de provenance de l'internaute, malgré tout le cheminement effectué par ce dernier sur de nombreux serveurs pour éventuellement arriver sur ceux de Yahoo !. Mais comme aucune solution n'est fiable à 100%, celle-ci comporte inévitablement une marge d'erreur. Pour preuve, l'affirmation faite depuis le site Web d'Infosplit que nous étions situés à Milan, alors que nous nous connectons depuis Paris. Sans doute était-ce parce que nous utilisions un fournisseur d'accès

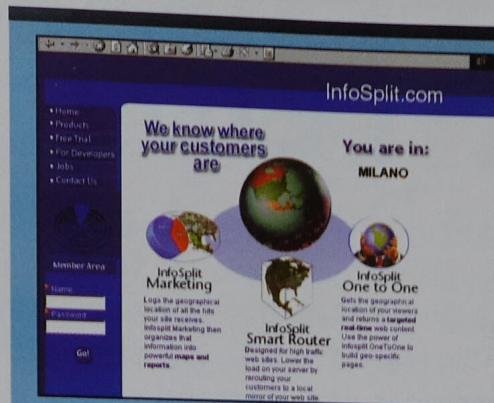
d'origine italienne (en l'occurrence 9 Télécom). Toujours est-il que la preuve est faite que même cette solution n'est pas entièrement digne de confiance.

Et quand bien même l'internaute serait localisé de façon certaine, il faudrait activer des programmes depuis les serveurs des sites visités pour détecter les contenus qui lui sont autorisés et ceux qui ne le sont pas. Yahoo ! estime qu'un tel travail nécessiterait l'emploi de 3000 personnes à plein temps, c'est à dire plus que tous les employés de la société dans le monde. De plus, il existe sur le Web de nombreux services et logiciels permettant de masquer la provenance de cette fameuse adresse IP. Il s'agit par exemple du site Anonymizer.com qui possède une solution très simple à mettre en œuvre puisqu'elle ne nécessite l'installation d'aucun logiciel particulier.

Il suffit de se connecter d'abord à leur site avant d'aller surfer librement, l'adresse IP s'affichant alors étant celle d'un de leurs serveurs - basés aux Etats-Unis - et non plus celle qui était la votre à l'origine et qui vous identifiait éventuellement comme internaute français. Cette solution est imparable. Que dire enfin des abonnés à AOL ? Les internautes français qui utilisent ce fournisseur d'accès (il sont environ 15%) passent automatiquement par des serveurs basés aux Etats-Unis. Ils ne pourraient être pris en compte si cette seconde famille de solutions technique était retenue par la justice.

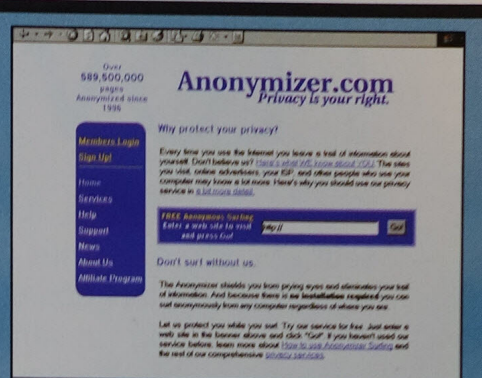
Il existe peut-être une dernière possibilité : celle offerte par les certificats numériques. Utilisés pour sécuriser les e-mails, ces véritables " passeports " des internautes pourraient servir à montrer patte blanche et prouver que l'on est bien autorisé à visiter le site demandé. Ceux des français empêcheraient l'accès aux enchères nazies. Les certificats numériques sont délivrés par des autorités certifiées comme Verisign ou Certinomis, filiale de la Poste et de Sagem. Mais leur mise en œuvre pour autre chose que des échanges de courrier électronique sécurisé demanderait une trop grande mise en œuvre technique pour tous les sites de la Toile mondiale et est donc très difficilement envisageable, pour l'instant ?

Finalement, la solution la plus sûre consisterait pour Yahoo ! à supprimer les contenus incriminés. Mais elle est impossible à mettre en œuvre, surtout aux Etats-Unis, au nom de la sacro-sainte liberté d'ex-



La société new-yorkaise Infosplit affirme posséder une solution permettant de détecter la provenance d'un visiteur à 95%. Nous avons dû tomber dans la mauvaise tranche puisque, alors que nous nous connectons depuis Paris, le site affirmait que nous étions milanais.

<http://www.infosplit.com>



Surfer avec une fausse adresse IP et cacher ainsi son pays d'origine ? Rien de plus facile avec des services comme celui d'Anonymizer.com. Cette solution imparable est de plus très facile à mettre en œuvre puisqu'elle ne nécessite l'installation d'aucun logiciel.

<http://www.anonymiser.com>

pression. Il faudrait surtout que la justice américaine se décide enfin à interdire la promotion et la mise en avant de tels objets. De leur côté, les responsables de Yahoo ! France ne peuvent pas non plus faire grand chose. Ils peuvent au mieux placer un avertissement sur les pages contenant des liens vers les enchères incriminées. Mais celles-ci sont de toute façon absentes du site Yahoo.fr. La justice souhaite même interdire à Yahoo ! France de placer sur son site portail des liens menant vers le site américain, car il est estimé que 200 000 clics mensuels y sont effectués. Mais tous ne concernent pas des liens menant vers les objets nazis mis aux enchères. De toute façon, n'importe qui peut directement taper yahoo.com sur son navigateur. Yahoo ! peut aussi expurger son moteur de recherche des mots et sigles en rapport avec le nazisme ou de tels contenus. Car aujourd'hui, il suffit simplement de taper " SS " sur le site d'enchères de Yahoo! US pour se retrouver directement sur une page proposant à l'encan les objets visés (lire notre encadré ci-contre).

De fait, sans doute vaut-il mieux tenter de responsabiliser les utilisateurs, plutôt que de vouloir s'acharner à mettre en œuvre des solutions techniques plus qu'aléatoires. Internet ne pourra jamais être contrôlé à 100%. C'est aussi à la justice de comprendre une telle évidence.

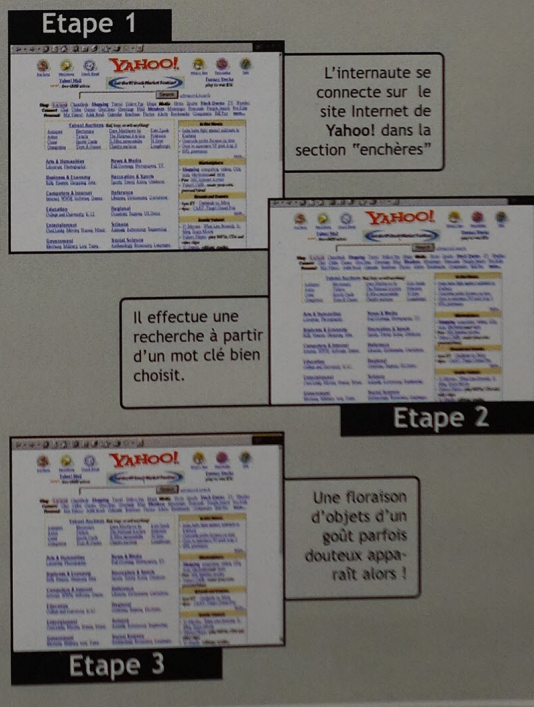
Pierre Chauveau

## Un accès très facile

L'accès aux pages des enchères de Yahoo ! où sont situés parfois des objets litigieux est on ne peut plus facile. N'importe qui y accède aussi aisément que s'il cherchait le dernier CD de Madonna ou PC d'occasion à acheter. Il suffit de se connecter au site Yahoo! US et de cliquer sur la rubrique des enchères (étape 1) pour arriver sur la page d'accueil des enchères.

Ensuite, une simple requête sur le moteur de recherche avec un mot bien ciblé (étape 2) vous emmène directement sur les pages incriminées par la justice française.

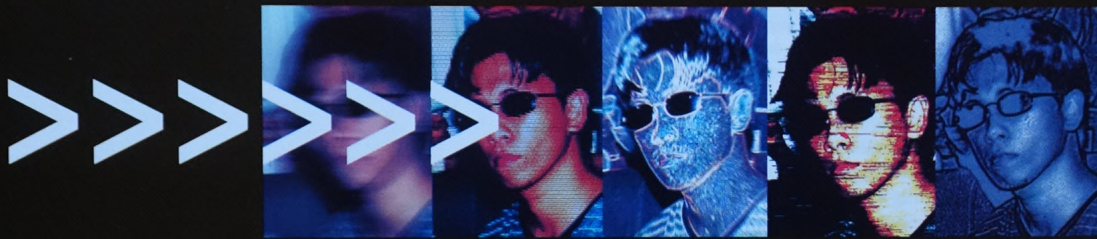
On y trouve aussi bien des décorations nazies que des dra-peaux, des affiches ou des casquettes d'officiers (étape 3). Des objets que possèdent beaucoup d'anciens combattants ou des collectionneurs. L'horreur est parfois accessible...



# I LOVE YOU...

Il y a quelques mois, ILOVEYOU s'affirmait comme le virus le plus destructeur et surtout, le plus médiatique de l'histoire. Son auteur présumé risque de passer de longues années derrière les barreaux. Une situation assez démesurée pour un simple fichier attaché qu'il était facile d'empêcher de se répliquer. Mais qui arrange pas mal de monde.

## Un message d'amour empoisonné



Onel de Guzman risque une peine de six à vingt ans de prison. Il devrait en effet être finalement inculpé et poursuivi par la justice de son pays, la police locale affirmant détenir assez de preuves de sa responsabilité dans la diffusion du virus ILOVEYOU, au mois de mai dernier. Ce philippin de 23 ans, ainsi que sa sœur et son compagnon, n'est cependant pas encore accusé d'être le "créateur" du virus. Après une première interpellation, quelques jours après le déclenchement de l'affaire, il avait d'ailleurs été relâché fautes de preuves. Mais le NBI (la police de l'île) a désormais besoin d'un coupable, subissant les pressions de certains Etats et organismes soucieux de relancer le débat sur la sécurité des réseaux. Guzman devrait être inculpé de violation de l'Access Device Regulation, une loi prohibant l'utilisation d'un élément matériel pour pénétrer par effraction dans un système de communications.

Rappelez-vous, c'était au mois de mai, le jeudi 4 exactement... Quatre heures après le début de sa diffusion, le virus ILOVEYOU faisait déjà la Une des agences de presse. C'aurait pu être le plus grand message d'amour jamais lancé de par le monde ; il ne répandit qu'horreur et destruction. Ce virus tire son nom du fichier joint qui l'accompagnait : Love-Letter-For-You.txt.vbs. Sous l'aspect d'un fichier texte on ne peut plus banal, se cachait en fait un programme destructeur réalisé en VBScript. La plu-

part des ordinateurs de la planète pouvaient être infectés puisque le virus fonctionnait sous Windows 98, 2000, mais aussi 95 et NT, à condition cependant pour ces deux derniers qu'Internet Explorer 5 soit installé. Les autres systèmes, comme MacOS ou Linux, ne pouvaient être touchés. Après réception par l'intermédiaire de n'importe quel logiciel de courrier électronique, il suffisait de cliquer dessus pour l'activer. A partir de là, un double processus s'enclenchait.

Tout d'abord, ILOVEYOU s'attaquait à certains fichiers présents sur le disque dur de l'ordinateur touché. Tous ceux portant, entre autres, une extension du type .vbs, .vbe, .css, .jpg, .gif, .vaw, .mp3, .doc, .xls, .html, etc. voyaient leur contenu remplacé par le code source du virus et leur extension changée en .vbs. A de rares exceptions près, ils étaient irrémédiablement perdus. Bien entendu, la base de registre de Windows était aussi touchée et modifiée, afin que le virus se déclenche à chaque redémarrage du système.

Ensuite, tous les systèmes infectés à partir des versions 98 et 2000 d'Outlook réagissaient en véritable centre de redistribution du virus. Celui-ci allait piocher dans le carnet d'adresses du logiciel de Microsoft pour se démultiplier et s'auto envoyer à tous les contacts enregistrés. D'autres logiciels, comme ceux destinés à l'IRC (Internet Relay Chat), étaient aussi utilisés pour la diffusion de ce virus. Si le montant total des pertes subies par les entreprises reste

difficile à estimer, plus de deux millions d'ordinateurs touchés ont vu le virus activé par leur utilisateur.

### Un vers mutant plus qu'un virus

D'ailleurs, faut-il parler de virus à propos de ILOVEYOU ? Dans le grand bestiaire de l'informatique (lire l'encadré ci-contre), ce fléau ressemble plus à ce qu'il est convenu d'appeler un vers, polymorphe qui plus est. Non seulement ce programme déclenche une action parasite ou destructrice (le but habituel d'un virus), mais il possède la faculté de se propager de lui-même par l'intermédiaire d'un réseau. Il le fait sans infecter un autre programme, mais simplement en trouvant une faille dans ceux présents sur le disque dur de l'ordinateur infecté. Internet, par l'intermédiaire des logiciels de messagerie et leurs interpréteurs de scripts, est donc son terrain de jeux préféré. Son qualificatif de polymorphe provient de sa capacité à muter, c'est à dire à "faire des petits" en se transformant.

Ce programme de mutation s'est d'ailleurs révélé très efficace. Une quinzaine de jour après l'apparition d'ILOVEYOU, plusieurs répliques semaient déjà la terreur dans le monde entier. Parmi eux, Resume Worm, qui détruisait les répertoires Mes Documents, Windows et Windows System, MotherDay, qui s'attaquait aux fichiers vitaux du système, comme ceux portant les extensions .bat, .ini et .com et surtout le virus NewLove. Mais pour avoir trop atti-

## Virus, vers ou troyens ?

Dans la famille des virus informatiques, il faut distinguer trois types de codes vicieux aux fonctionnements et méthodes de reproduction différents.

Il y a tout d'abord le virus proprement dit. Il s'agit d'un programme, ou d'un pan de programme, dont la principale faculté est de se répliquer pour se répandre de poste à poste. Pour cela, il se glisse à l'intérieur d'un autre fichier et opère lors de l'utilisation de celui-ci. Il peut aussi se nicher dans le secteur de démarrage d'une disquette ou d'un disque dur. Certains sont totalement inoffensifs et se contentent d'afficher des messages ou de changer les noms de certains fichiers. Mais les plus dommageables sont capables d'effacer en quelques secondes le contenu de tout un disque dur.

Viennent ensuite les vers, du type

d'ILOVEYOU. Alors que les virus classiques ont besoin de l'action d'une " personne tierce " pour se reproduire et infecter d'autres postes, ceux-ci le font de manière autonome en exploitant les failles et les fonctionnalités de certains logiciels. Ils peuvent notamment se transmettre par l'intermédiaire du courrier électronique. Avec l'avènement d'Internet, ils trouvent un terrain de jeu à la mesure de leurs capacités.

Enfin, troisième catégorie, les chevaux de Troie : le virus ne se cache plus puisqu'il s'agit d'un programme à part entière, qui apparemment est inoffensif et possède même une utilité. Il peut s'agir par exemple d'un petit jeu. Mais sous sa forme bienveillante, il attend patiemment son heure pour dévoiler son mauvais côté (souvent destructeur) au moment où l'on s'y attend le moins.



**Onel de Guzman**  
étudiant de 23 ans  
Philippin



ré l'attention sur lui, notamment par son pseudo proche de celui du virus originel, ce dernier fit beaucoup moins de dégâts qu'il n'aurait pu en faire. Les gens avaient appris à se méfier des messages d'amour.

### D'inévitables failles chez Microsoft

Dans les jours suivants cette attaque, trois types d'acteurs se partageaient le devant de la scène médiatique. Le FBI, qui recherchait l'auteur du virus, les éditeurs de logiciels antivirus, qui affirmaient tous détenir la solution au problème, mais aussi (et bien sûr) Microsoft.

Celui par qui le mal se répand ! Tel est la réputation que s'est une fois de plus taillé le géant de Redmond. C'est sur ses systèmes d'exploitation uniquement que le virus était actif. C'est par l'intermédiaire d'un de ses logiciels qu'il se répandait à la vitesse de la lumière dans les systèmes de messagerie du monde entier. C'est tout de même un peu logique quelque part. Un auteur de virus recherche avant tout la gloire et la célébrité pour son " œuvre ". Il a donc tout intérêt à fabriquer un programme s'attaquant au plus grand nombre d'ordinateurs possible. Ceux fonctionnant grâce aux logiciels de Bill Gates sont donc des cibles toutes trouvées. Cependant, le travail des virus est grandement facilité par les innombrables failles de sécurité dont ils sont affublés. En l'occurrence, Outlook contenait une " back door ", ou porte de derrière, laissant un libre accès pour le virus à son carnet d'adresses.

Microsoft a rapidement mis en place un correctif téléchargeable depuis son site Web. Une fois installé, il interdisait l'envoi et la réception en tant que pièces jointes de certains fichiers ainsi que la navigation sur certains sites Web exécutant ce type de fichiers à la connexion. Pas très pratique il faut l'avouer. De plus, le logiciel Exchange, utilisé comme serveur de messagerie par de nombreuses entreprises, ne comporte pas de filtres stoppant la propagation de messages contenant certains en-têtes spécifiques (au contraire d'Outlook). Au final, c'était au destinataire final de s'entourer de prudence et de faire en sorte de ne pas ouvrir le fameux message infecté.

De leur côté, les éditeurs de logiciels antivirus n'ont vraiment pas tardé à réagir. Mais pour quel résultat ? Bien souvent, en effet, le mal était fait. Si la plupart se vantaient d'avoir fourni une réponse à ILOVEYOU en quelques heures, cette affaire aura mis une fois de plus en relief leur incapacité à lutter contre des virus inconnus, même s'ils sont mis à jour quotidiennement. La plupart d'entre eux se basent en effet sur des fichiers de signatures (la marque des virus) connus, provenant de virus déjà répandus. Quand un nouveau virus est créé, ils ne peuvent reconnaître son intrusion dans le système. Seuls quelques logiciels, comme Viguard de Tegam ou ADInf de Safe Work, se passent de ces bases pour fonctionner. Ils tentent de détecter des modifications ou des mouvements suspects à l'intérieur de fichiers

ou de programmes. Si ces mouvements peuvent provenir de virus, il arrive bien souvent que ces logiciels tirent la sonnette d'alarme pour des broutilles. Bref, aucune solution n'est vraiment fiable à 100%. Mais à chaque fois, les éditeurs de logiciels antivirus réussissent à faire parler d'eux et à vendre de nombreux exemplaires de leurs produits. Ils attirent aussi un grand nombre d'internautes, tous désireux de télécharger la dernière mise à jour sortie, sur leur site Web. Un nouveau virus de type ILOVEYOU représente pour eux un bon moyen de se faire de la publicité à moindres frais.

Enfin, le FBI s'est immédiatement mis en chasse du ou des auteurs du virus. C'est dans la confusion la plus totale que les premières rumeurs ont amené les policiers américains à arrêter une première fois Onel de Guzman et ses deux complices présumés. Un jeune suédois, Jonathan James, chasseur de pirates à l'occasion, leur avait fourni des renseignements concordants. C'est déjà lui qui avait contribué quelques mois auparavant à l'arrestation de David Smith, l'auteur du virus Melissa. L'état de panique généré par l'apparition d'ILOVEYOU et les dégâts financiers qu'il a provoqué justifient pour les forces fédérales l'utilisation de moyens pratiquement illimités pour lutter contre lui et ses auteurs. L'occasion aussi de préserver leurs grands systèmes d'espionnage du Réseau mondial des attaques des partisans d'un Internet libertaire.

# ENTREVUE

[ Ian Hall-Beyer ]

Membre de l'équipe Gnutella

## Gnutella

Ian, connu dans certains cercles sous le pseudo de "manuka", est ce qu'on peut appeler un accro de l'informatique.

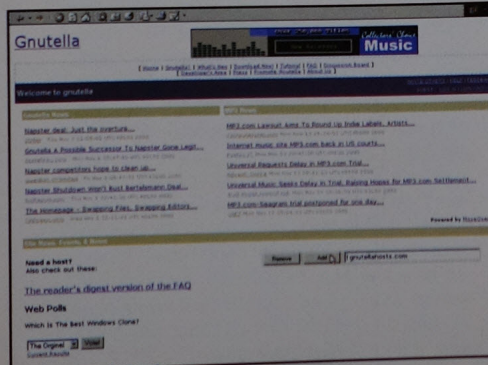
Au cours des quatre dernières années, il a été consultant spécialisé dans l'administration et la gestion réseau des systèmes Unix. On a pu compter parmi ses clients des sociétés telles que MCI (3ème opérateur téléphonique aux Etats Unis), IBM ou General Electric.

Il travaille désormais dans la division éducation de Sun Microsystems (à l'origine notamment du langage Java.) Sa contribution la plus notable à la communauté Linux reste le firewall ipchains qui est utilisé par plusieurs milliers d'internautes et de sociétés.

Dans ce qui lui reste de temps, il s'occupe en partie de [www.langistix.com](http://www.langistix.com) et de [www.nerdherd.net](http://www.nerdherd.net)

Il vit à Boulder, Colorado, où il partage un appartement avec deux autres accros de l'informatique, une myriade de chats et un nombre inhabituel d'ordinateurs...

<http://gnutella.wego.com>



## L'interview exclusive

>> Comment et quand avez vous rejoint l'équipe de Gnutella ?

L'équipe en tant que tel est très informelle, nous sommes séparés par la géographie (je suis à Denver, Nathan est à Seattle, Gene et Spencer sont à San Francisco). L'équipe s'est formée rapidement après le dévoilement du programme original, qui a été rapidement censurée par AOL, qui contrôle Nullsoft.

Nathan est à l'origine du site web, et je lui ai donné de l'espace sur mes serveurs et ma ligne T1 (1.544 Mbps). Gene demeure avec certains membres de l'équipe Nullsoft, et Spencer est un de ses amis.

Après quelques semaines, ma ligne et mon serveur commençaient à craquer sous la pression des milliers de visiteurs au site. Gene travaillait à ce moment là pour la société Wego.com, et celle ci a alors proposé de nous héberger.

>> L'équipe a l'air jeune, quelle est l'atmosphère qui règne au sein de celle ci ?

Nous sommes tous des amateurs et des professionnels en technologie, et cela crée une atmosphère tout à fait agréable. Tout le travail sur le site et la coordination se font en-ligne, par courrier électronique ou par IRC<sup>(1)</sup>.

>> Quelle est votre participation dans la création et/ou le développement de Gnutella ?

Ma participation se limite au développement du site même. Je ne suis pas un programmeur. Gene et Spencer ont fait un client qui fonctionne sur le réseau Gnutella, pour les systèmes Unix.

>> Quelles sont les conséquences de "l'affaire Napster" pour Gnutella ?

Les conséquences immédiates: 1 million de visites sur le site dans la semaine autour de la fermeture du service de Napster. Depuis que l'injonction est levée, le trafic est beaucoup moins fou :)

Les conséquences à long terme: J'imagine que RIAA essaiera d'attaquer quelqu'un pour Gnutella. Ils auront beaucoup de difficulté trouver ce quelqu'un, vu que Gnutella est simplement un concept technologique. Il n'y a pas de société ou d'entité légale qui le contrôle.

>> Gnutella est gratuit, la société éditrice trouve t'elle une rémunération, et comment ?

Aucune. Il y a de la publicité sur le site, mais tous ces revenus vont directement à Wego pour payer, dans la mesure du possible, les ressources que notre site demande (hébergement, bande passante, etc.)

>> Quelles sont les grandes différences de Gnutella vis à vis des autres logiciels Peer to Peer<sup>(2)</sup> ?

Je ne suis pas très familier avec les autres logiciels, donc je ne peux pas vraiment donner de commentaire concret :)

>> Quelles sont les prochains pôles de développement de Gnutella ?

Tout d'abord trouver des méthodes pour agrandir le réseau - mais dans l'immédiat, il y a beaucoup de problèmes lorsque le trafic devient trop lourd. Après ça, un groupe essaiera de développer un protocole de deuxième génération qui devrait fonctionner beaucoup mieux.

Nous tenions à remercier Ian qui bien que n'ayant pas pratiqué le français depuis 7 ans (sa langue maternelle) a accepté de répondre à nos questions en français.

(1) IRC : . Protocole conçu pour dialoguer à plusieurs sur des serveurs spécifiques en temps réel

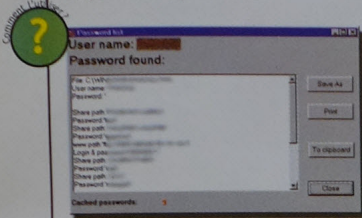
(2) Peer to Peer : Dans la lignée de B to C (Business to Client), P to P signifie de "Point à Point" ou autrement dit directement entre deux internautes.

# LOGICIELS

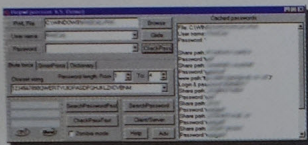
## [ Mots de passe Windows ]

### PwlTool

Version : 6.5  
Système : Windows 3.1/95/98  
Poids : 374 Ko  
Prix : Shareware  
Les + : Interface très réussie et complète  
Les - : Payant pour la version finale  
Note : 5/5  
<http://soft4you.com/>



1 L'interface paraît assez chargée mais la version de démonstration est limitée au strict minimum.



2 Vous pouvez imprimer ou copier les données récupérées dans le presse papier pour les réutiliser avec un autre logiciel

### Mots de passe à gogo !

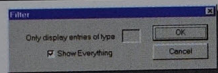
Le système d'exploitation de Microsoft, Windows, a la fâcheuse tendance de stocker un certain nombre de mots de passe dans un fichier propre au système Windows ayant comme extension .pwl. Celui-ci peut s'avérer être un véritable maillon faible permettant à quelqu'un de mal intentionné d'éventuellement utiliser votre messagerie, votre ordinateur et d'accéder à certains sites protégés avec votre identité. Bref une véritable faille qui a toutefois ses bons côtés puisqu'en cas d'oubli d'un de vos mots de passe vous avez toujours l'espoir de le retrouver par l'intermédiaire de ce fichier .pwl, tout simplement en utilisant les logiciels que nous allons vous présenter !

Il existe un grand nombre de produits permettant en théorie d'exploiter ce fichier, pourtant vous vous rendez compte rapidement que nombre d'entre eux sont inexploitable ou corrompus.

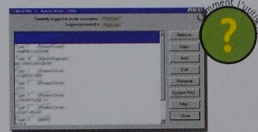
Trois logiciels ont particulièrement retenu notre attention:  
PwlTool 6.5 / WinPWL 3 / Password Stealer 1.6

### WinPWL

Version : 3  
Système : Windows 95/98  
Poids : 52 Ko  
Prix : Gratuit  
Les + : Filtres, compatible Windows Me (version 3.5)  
Les - : Fenêtre non redimensionnable  
Note : 4/5  
[www2.memlane.com/aklotz/](http://www2.memlane.com/aklotz/)



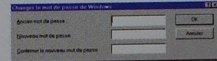
4 Un filtre simpliste



1 Lancez Password Stealer puis cliquez sur "Get Passwords" et la liste apparaît...

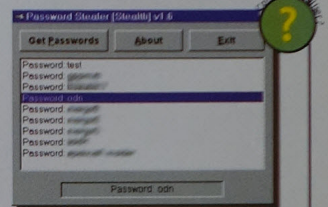
2 Configurer un accès réseau Netware, une connexion Internet ou un compte à un site Web.

3 Un clic et vous pouvez changer le mot de passe utilisateur.

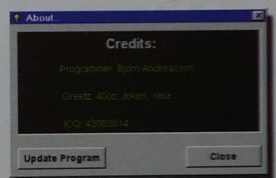


### Password Stealer

Version : 1.6  
Système : Windows 3.1/95/98  
Poids : 32 Ko  
Prix : Gratuit  
Les + : Poids ridicule, rapide et se glisse partout  
Les - : Récupération des mots de passe pas des identifiants utilisateurs  
Note : 2/5  
<http://industries.progenic.com>



1 Lancez Password Stealer puis cliquez sur "Get Passwords" et la liste apparaît...



2 Pour connaître les dernières mises à jour

## Interview avec Aaron Klotz Créateur de WinPWL

Aaron Klotz vit à Medicine Hat dans l'état de l'Alberta au Canada. A peine âgé de 18 ans, il est tombé à l'âge de 7 ans dans l'informatique en commençant à programmer en BASIC pour passer au C/C++ à 13 ans. Bref vous l'avez compris, il s'agit de ce que l'on appelle un jeune homme précoce...

> > Que faites-vous actuellement ?

Je rentre en première année d'université en section informatique. Pour payer mes études je travaille en parallèle dans un magasin de micro.

> > Pourquoi avoir développé WinPWL ?

Je cherchais un outil simple d'administration système. Au département où je travaille, nous sommes régulièrement confrontés à des personnes qui oublient de nous donner leurs mots de passe pour se connecter à Internet lorsqu'elles nous laissent leur ordinateur. Ces mots de passe nous servant à vérifier que la personne pourra bien se reconnecter après que nous ayons réparé la machine.

Nous essayons systématiquement de téléphoner à ces personnes mais elles sont tellement paranoïaques qu'elles refusent de nous donner leurs mots de passe. Aussi, comme bien souvent ceux-ci sont stockés dans les fichiers PWL. Je voulais donc un logiciel pour pouvoir les lire en toute simplicité et ce, gratuitement.

> > Comptez-vous faire une version pour Windows Millennium et éventuellement un nouveau programme pour NT ?

Une nouvelle version pour Millennium est en cours. Elle est en phase de test et devrait voir le jour d'ici quelques semaines. Je travaille par ailleurs sur la possibilité à d'autres programmeurs de développer des plug-in pour WinPWL. Mais il faut bien avouer que j'ai peu de temps à y consacrer actuellement. Je ne suis pas réellement intéressé par NT dans l'immédiat. WinPWL est destiné aux environnements Windows 95 ou 98 et, à moins que Microsoft décide finalement de combiner Windows 9x avec NT, je n'ai pas prévu de redévelopper une version spécifique à NT.

**Pirates informatiques**

**Hacking**

**Intrusion**

**Cryptographie**

**Securite**

**Attaques**

**Virus**



**Des dizaines de news, des interviews,  
des dossiers couvrant toute l'actualite  
du milieu underground et alternatif.**