

TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

0% DE PUBLICITE  
JUSTE DES ARTICLES  
2,00 €

www.hackmag.com  
**HACKER**  
news  
**Magazine**

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

**HACKING  
DELICIOUS**



L'un des plus gros **SITES**  
**AMÉRICAINS MENACÉ**

**PROTÉGER**  
VOTRE CLEF USB / DVD  
DES REGARDS INDISCRETS

**MEDIADEFENDER**

le plus **GRAND SCANDALE**  
sur l'**ÉCHANGE DE FICHIERS**

**L'AUTRE VISAGE  
DE LA MULE**



une **VERSION MEILLEURE**  
que l'original...



**LES PACKS LOGICIELS  
100% PIRATES ARRIVENT !**

Des **CD COMPLETS** prêts à l'emploi pour **PIRATER**

Année 4 - n° 21 Bimestriel  
décembre 2007 - janvier 2008

Lamer ('lae'mr)

Aspirant cracker, aux capacités et connaissances informatiques limitées, souvent maladroit et disposé à mener des actions douteuses et nuisibles.

Hacker News Magazine  
Et son complice italien  
Hacker Journal  
1ers magazines européens Hacker

Boss: TheGuilty@hackerjournal.it

Les camarades de la rédaction européenne :  
Gregory, Fred, Damien Bancal,  
One4Bus, Max. G. Tronconi,  
K2der, Sylvain, Silvio De Pecher,  
Contents by MDR.

Traduction et adaptation :  
Laurent et Sylvie Arsenau

Mise en page :  
Selestudio

Couverture:  
Daniele Festa

Editeur :  
WLF Publishing SRL  
Via Donatello 71  
00196 Roma

Imprimeur : Roto 2000,  
Via Leonardo da Vinci 18/20  
Casarile (MI) Italy

Distribution:  
MLP - 55 bd de la Noirée  
ZA de Chesnes  
38070 St Quentin Fallavier

Directeur de la publication :  
Teresa Carsaniga

Dépôt légal : à parution  
ISSN : en cours

Copyright WLF Publishing

Les droits sont réservés et protégés  
Pour la version imprimée.

La rédaction n'est pas responsable des  
textes, documents, photos, dessins qui lui  
sont communiqués et n'engage que la  
responsabilité de leurs auteurs.

Sauf accord particulier et publiés ou non, ils  
ne sont pas renvoyés.

Les indications de prix et d'adresses  
sont de l'information fournie sans  
aucun but publicitaire.

# Editorial

HACKER  
Magazine

## Nous sommes tous des lammers!

*"Grand est celui qui, dans la sagesse de ses années, a su  
conserver un cœur d'enfant-  
Anonyme*

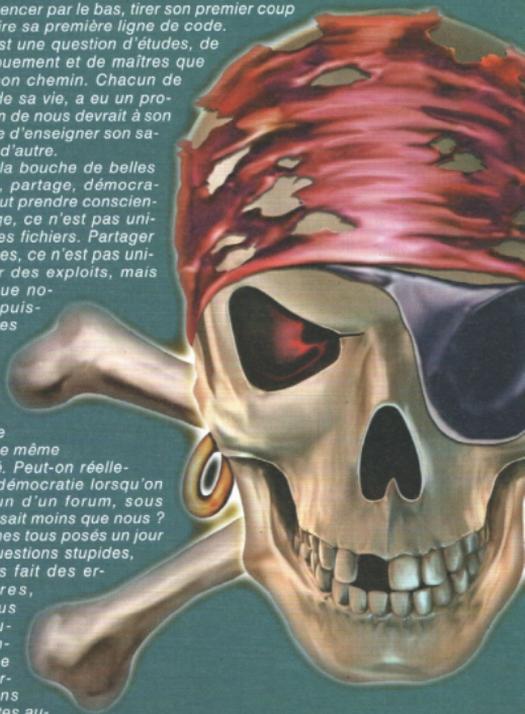
*Ou peut-être pourrions-nous dire «celui qui a su conserver un cœur de lamer». Partons d'une thèse reconnue : chez l'homme, ce qui fait la différence entre un champion et un bon joueur, c'est le talent. S'il n'existe qu'un seul Pelé dans toute l'histoire du football, chaque joueur peut et doit briger une carrière à la Trezeguet.*

*Ainsi, une fois le talent mis de côté, tout ce que l'on peut faire, c'est commencer par le bas, tirer son premier coup de ballon ou écrire sa première ligne de code.*

*Ensuite, tout est une question d'études, de volonté, de dévouement et de maîtres que l'on trouve sur son chemin. Chacun de nous, au cours de sa vie, a eu un professeur et chacun de nous devrait à son tour faire en sorte d'enseigner son savoir à quelqu'un d'autre.*

*On se remplit la bouche de belles paroles : liberté, partage, démocratie etc., mais il faut prendre conscience que le partage, ce n'est pas uniquement celui des fichiers. Partager ses connaissances, ce n'est pas uniquement publier des exploits, mais faire en sorte que notre*

*expérience puisse former d'autres personnes qui pourront ensuite participer au sharing. La liberté, c'est faire en sorte de donner sa chance même au dernier arrivé. Peut-on réellement parler de démocratie lorsqu'on bannit quelqu'un d'un forum, sous prétexte qu'il en sait moins que nous ? Nous nous sommes tous posés un jour ou l'autre des questions stupides, nous avons tous fait des erreurs grossières, nous avons tous perdu des heures de programmation à cause d'une simple erreur, nous avons tous eu des doutes auxquels nous n'avons pas su faire face, nous avons tous rencontré des problèmes que quelqu'un nous a aidé à résoudre... bref... nous avons tous été des LAMERS !!!*



NO COPY

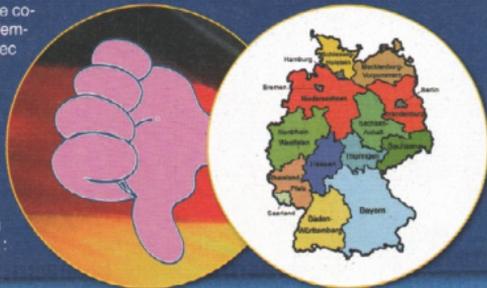
NO PARTY

**M**ais que se passe-t-il en Allemagne ??? Bon nombre d'entre vous répondront tous en cœur "qu'est-ce que ça peut bien nous faire !!!" Pourtant, il y a de quoi s'inquiéter, car si nous suivons les traces de l'Allemagne, nous pourrions bien dire adieu à notre liberté. Le mois dernier, le Bundsrat (l'une des deux chambres du Parlement allemand) a en effet approuvé une loi interdisant toute copie de films et de musiques, même en vue d'une simple sauvegarde. Vous n'aurez donc aucun mal à comprendre toute l'ampleur de cette loi... En pratique, cela signifie que si j'achète le dernier CD des Nine Inch Nails (et nous ne parlons pas d'eux par hasard), non seulement je ne pourrai pas m'en faire une copie sur CD pour l'emporter partout avec moi de façon à ne pas abîmer l'original, mais je ne pourrai pas non plus le copier sur mon ordinateur ou sur mon lecteur Mp3 ! Je n'ai donc aucun droit :

juste celui d'acheter le CD, de l'écouter et s'il se détériore, de le racheter... De même pour les films. Cette mesure a soulevé un large flot de contestations au sein des associations de consommateurs et même chez certains partis minoritaires. Car elle vise également l'IpTv et les programmes télévisés. Le gouvernement allemand a ainsi déclaré vouloir se conformer, à travers cette loi, aux directives communautaires. Mais, quelle mouche les a donc piqués ? Car à franchise parler, cette loi nous semble totalement démesurée. Partons de quelques hypothèses : tout d'abord, si j'achète un album et que je souhaite l'écouter sur mon lecteur Mp3, que dois-je faire ??? D'après la loi, je ne peux pas copier le

CD sur mon lecteur. Je devrais donc me connecter sur des sites de musique Mp3 et le télécharger on-line...

Deuxièmement, comment faire pour prouver que les Mp3 que j'écoute sur mon lecteur ont été achetés en toute légalité ? Dois-je me balader avec tous les reçus ? En outre, lorsque je télécharge un fichier Mp3 sur un site, je dois alors le télécharger directement sur mon lecteur car si je le télécharge sur mon PC puis sur mon lecteur, je serais en train d'en faire une copie. Bref, une loi on ne peut plus idiote ! En toute honnêteté, espérons que cette fois au moins, nos politiciens feront preuve d'un peu de bon sens pour ne pas adopter une telle loi, si injuste et inutile. Car nous ne croyons absolument pas qu'elle mènera à une réelle diminution du piratage. Elle ne servira qu'à échauffer les esprits et à éloigner davantage les jeunes de la légalité et de la musique. ■





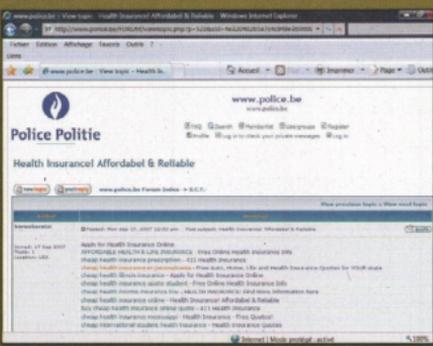
## POUTINE PRÉPARE LES ÉLECTION

L'Union des forces de droite russe (SPS) accuse le Kremlin, donc le gouvernement de Vladimir Poutine, d'avoir organisé une attaque informatique à l'encontre de son site Internet, www.sps.ru. Mission de cette soit disant attaque électronique, bloquer la page web du SPS, quelques semaines avant les législatives. Une attaque qui empêche toutes visites. Ce parti d'opposition russe a trouvé ce moyen de faire parler de lui en accusant Moscou d'avoir organisé cette cyberattaque. Un piratage DoS, avec 6 000 connexions à la seconde, lancée à partir de 400 IP différentes.

# DU CUL ET DES CASINOS

Le forum du site Internet officiel de la police Belge, Police.be, a été la visite. Il a été découvert, à la mi-novembre, que l'ensemble du forum avait été envahi de messages publicitaires pas comme les autres. Alors que l'on aurait pu imaginer tomber sur les derniers articles de loi et autres messages liés aux actions de la police Belge, les visiteurs tombaient sur des listes de médicaments, sur des centaines de liens dirigeant vers des sites pornos et autres casinos en ligne. Des dizaines de

milliers de liens, dans chaque page de ce forum. Cette invasion sembla être l'œuvre d'un code malicieux ayant exploité, en septembre dernier, une faille dans le forum. Rapidement prévenu, le forum a été retiré du site officiel de la police belge.



## LA NSA ESPIONNE INTERNET VIA AT&T

La chaîne MSNBC a révélé le témoignage d'un technicien de chez AT&T, opérateur téléphonique historique US. Il a indiqué que la NSA (National Security Agency) recevait des copies de l'intégralité des communications passant par AT&T. Appels téléphoniques, emails et trafic Web, nationaux et internationaux. La NSA

a installé ses e-espions à San Francisco, Los Angeles, San Diego, San Jose et Seattle.



## MORT DU TOP WAREZ HPN

La police a mis fin aux agissements d'un top warez baptisé HPN. La police polonaise a fermé, jeudi 8 novembre, un serveur informatique utilisé pour diffuser illégalement des albums de musique avant que ces derniers ne soient officiellement mis en vente dans les commerces. Les policiers ont saisi aussi du matériel dans les locaux de l'université de Wrocław dont six serveurs contenant pas moins de 37 disques durs (12 To). Deux person-

## HOT NEWS

### DE L'ARGENT GRÂCE AUX FAUTES DE FRAPPES SUR INTERNET

Les clients de l'opérateur Internet Américain Verizon font gagner de l'argent à leur FAI à chaque fois qu'ils se trompent dans une adresse Internet. Les clients sont renvoyés sur une page de recherche, baptisée "Advanced Web Search", une page contenant des publicités. Un moyen de gagner plusieurs milliers de dollars supplémentaires en profitant des doigts crochus des clients. En 2003 déjà, Verizon avait déjà mis en place ce système. A l'époque, l'ICANN avait exigé que cesse cette redirection.

### UN VIRUS INFORMATIQUE S'INVITE À L'HÔPITAL

David Farr travaillait pour l'hôpital St. Francis d'Indianapolis. Il était le seul homme de ce service et partageait une chambre avec quatre autres personnes féminines. Au milieu de ce espace de repos, un ordinateur commun. En octobre 2000, découverte que le bookmark du monsieur était rempli de liens pornos. Faute grave pour la direction de l'établissement qui va mettre le docteur à la porte. 7 ans après, un expert a conclu qu'un virus informatique était passé par là.



### 100 SERVEURS TRACKERS TORRENTS SAISIS

Une centaine de serveurs ont été saisis par les policiers Hongrois, le 8 novembre. Ils servaient de trackers bittorrents pour le portail le plus populaire de ce pays, bitHumen (30.000

adherents). L'ensemble des domaines utilisés pour ces trackers ont été fermés. Cette saisi a eu un autre effet dans le pays. Le trafic est passé de 60 à 35 Gbits par seconde.



## LA GENDARMERIE

### NE CHASSE PLUS

### LES PETITS COPIEURS

La Gendarmerie Royale du Canada (GRC) n'enquête plus, depuis plusieurs mois, sur les internautes qui téléchargent illégalement de la musique sur Internet. Le journal Canadien « le Devoir » indique que la GRC n'a pas assez d'hommes, de moyens et de temps pour enquêter sur les copieurs de Mp3. La tâche est tout simplement trop lourde. Le nombre d'internautes qui téléchargent de la musique est trop important.



nes ont été arrêtées. Au moment de l'action HPN accueillait plus de 11,000 albums MP3 complets et autres CDs promotionnels. Parmi les groupes affiliés à ce top site warez se trouvaient d'importants groupes comme SAW ou encore RAZOR1911.

### VIRUS VENDUS AVEC DES DISQUES DURS NEUF



Le constructeur de disque dur Américain Seagate a découvert que des disques durs, qu'ils faisaient fabriquer en Chine, avait été piégé avec des Chevaux de Troie. Les disques durs externes ont été commercialisés à Taiwan. En septembre, un virus avait été pré-installé dans des Seagate Maxtor 3200. Des HD vendus aux Pays-bas.





# OÙ SONT LES CYBER-TERRORISTES ?

Début novembre, une attaque d'envergure d'Al-Qaeda avait été annoncée par un site israélien. Une attaque visant des sites Internet importants. Pas de nom, pas de cible précise, mais une grande peur qu'aime tant orchestrer les américains. Le site en question indiquait avoir les preuves qu'une attaque de type DoS, allait être orchestrée à partir d'un logiciel diffusé par les jihadiste. Une programme du nom d'Electronic Jihad Program. Cette attaque devait se dérouler le 11 novembre.

## LA MISE À JOUR DE L'IPHONE DÉJÀ OBSOLETE FACE AUX PIRATES

À peine sorti en Europe en version firmware 1.1.2, l'iPhone se retrouve de nouveau mis à mal par des hackers. Afin de pouvoir profiter d'une version désimlockée du téléphone d'Apple, il faut effectuer un "downgrade" de l'iPhone version firmware version 1.1.2 vers la version 1.1.1 grâce à un outil nommé iPhuc. Beaucoup de manipulation qui pourrait, pour les doigts crochus, faire planter définitivement le téléphone de la grosse pomme. Les étapes sont encore assez complexes, mais les groupes de hackers travaillant sur le "jailbreak" préparent une interface d'installation simplifiée. Le paquet "Installer.app", fournit par les hackers de jailbreakme.com, permet d'installer OktoPrep. Le mode d'emploi complet est proposé sur leur site.



## UN VIRUS DANS DES PAGES MYSPACE

Un cheval de Troie a été caché dans des pages MySpace. Plusieurs artistes, dont Alicia Keys ont vu leurs pages ainsi piégées. Des pirates aient trouvé le moyen d'infecter les visiteurs à partir des pages de cet espace communautaire. Les pirates, qui utilisent des adresses en Chine et aux Pays-bas, ont déjà piégé les blogs de la star R'n'B Alicia Key. Une attaque assez simple, en fait, elle serait liée à l'opération "Myspays" lançait au début du mois de novembre. Des pirates informatiques avaient rendus disponible sur Internet 62 000 login et mots de passe de comptes d'utilisateurs MySpace. Les pirates ont eu simplement à rajouter un iframe dans chaque page. Iframe qui téléchargeait à chaque visite un virus espion dans les ordinateurs des visiteurs.



## DES BLOGS À L'ASSAUT D'UNE ARNAQUE PHARMACEUTIQUE

En octobre, des milliers de blogueurs russes se sont unis pour combattre une escroquerie pharmaceutique. L'escroquerie portait sur un pseudo médicament anti arthrite.

Le prix initiale pour ce type de médicament peut valoir jusqu'à la moitié d'une retraite mensuel-

le en Russie. Des centaines de clients ont acquis ce remède qui n'était qu'une arnaque. Des blogueurs ont lancé une alerte. Bilan, 21 millions d'appels téléphoniques ont été passés afin de bloquer le commerçant indélicat.



## DES PIRATES S'ATTAQUENT AU FIRST FORENSIC FORUM

Une groupe de hackers, 4udit-S3curity-T3rror, est passé par le site Internet des britanniques du First Forensic Forum, F3.org.uk, une association de professionnels de la sécurité informatique. Si le piratage de site est devenu une chose banale sur la toile, la cible l'est beaucoup moins.

## HOT NEWS

### UN PIRATE RISQUE 60 ANS DE PRISON POUR DIFFUSION DE TROYEN

John Schiefer, un Américain de 26 ans, se disait être un consultant en sécurité informatique. Fort de son "expérience", il va convaincre plusieurs entreprises Américaines et étrangères de ses capacités à les protéger des assauts des pirates, hackers et autres virus informatiques. Sauf que John avait un petit secret qu'il vient de révéler à un juge Californien. John Schiefer et des amis rencontrés sur Internet piégeaient les machines de ses clients. Surveiller les faits et les gestes de ces derniers. Et quand cela était possible, les pirates intercepter leurs données bancaires et allaient se servir directement dans les caisses de leurs victimes. L'arnaque, explique le F.B.I. En charge de l'enquête, lui a offert la possibilité d'installer 250 000 chevaux de Troie, des logiciels espions, dans autant d'ordinateurs infiltrés. L'agence de Presse Reuters Indiquait, au moment du jugement, que le pirate informatique aurait, lui et ses complices, réussi à piéger et voler, entre autre, une agence de publicité Néerlandaise. Les publicitaires vont se faire détourner la coquette somme de 20.000 dollars (Un peu plus de 13.000 euros). Pas très discret, c'est d'ailleurs ce qui va perdre John et ses complices, John Schiefer a été arrêté et vient de plaider coupable devant un tribunal Californien. Il risque 60 ans de prison et une amende salée 1,75 millions de dollars. Voilà qui devrait lui laisser le temps de réfléchir.



## AYYILDIZ OWNED

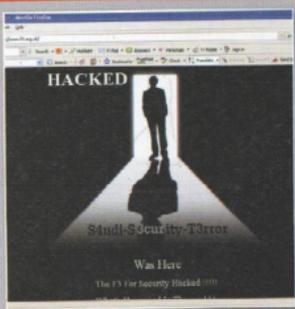
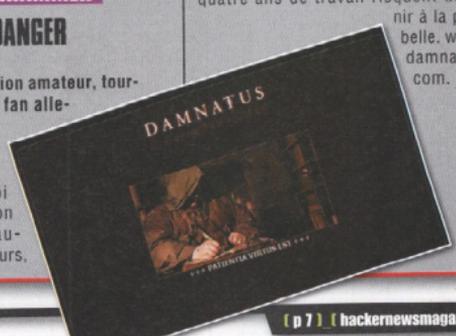
L'un des plus important groupe de pirates informatiques Turcs, Ayyildiz piratés. La guerre numérique lancée par ce groupe a, semble-t-il, tapé sur le système de plusieurs hackers, dont des Suédois. chauffer les joues et les souris d'un certain nombre de hackers. Bilan, le serveur ou était installé le forum de Ayyildiz a été piraté. Les intrus ont sorti une base de données avec noms, ip, mails, mots de passe, adresses MSN... Elle pèse près de 5 Mo et contient, entre autre 47,643 lignes de données. Pour rappel, ce groupe avait lancé une attaque numérique contre plusieurs milliers de sites suédois à la suite de la diffusion, dans la presse, d'une caricature du Prophète Mahomet.



### LE FILM WARHAMMER 40000 EN DANGER

Cette production amateur, tournée par des fans allemands de ce jeu, risque de ne jamais sortir en raison de la loi sur la protection des droits d'auteurs. Onze acteurs,

un budget de plus de 10.000 euros et quatre ans de travail risquent de finir à la poubelle. [www.damnatus.com](http://www.damnatus.com).



# LE PIRATAGE, un jeu d'enfant ?

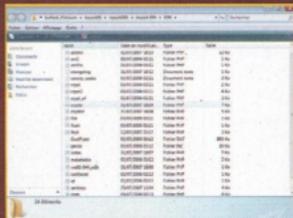
*Sur Internet, il a toujours existé des outils de piratage « clic and hack ». Si certains aiment cracher sur ce type d'outil, force est de constater qu'ils ont le vent en poupe. Voici quelques exemples de « prêts à l'emploi » qui laissent froid dans le dos et qui présagent un avenir sur la toile des plus inquiétant.*

**L**es packs, voilà un fléau difficilement contrôlable. Alors qu'il existe depuis très longtemps des outils permettant de générer automatiquement et sans connaître le moindre code de programmation, l'apparition depuis quelques mois de packs laissent une véritable inquiétude planer sur nos ordinateurs.

Les logiciels à la mode du moment se nomment Mpack, Icepack, Shark, Fishing\_Bait, ...

## :: MPACK, la framework attitude

Alors que les outils de piratage « clic and play » pullulent sur le réseau des réseaux, pour la première fois, des pirates mettent en place un tout en un qu'ils commercialisent. La mode des packs est lancée et elle n'est pas prêt de s'arrêter !



Souvenez-vous, nous sommes à l'époque en mai 2007. Plusieurs milliers de



serveurs italiens, près de 10.000 tombaient sous les coups de pirates informatiques. 500.000 internautes victimes d'un étrange mal baptisé Mpack. Mpack est un framework, comprenez qu'il bosse avec un ensem-

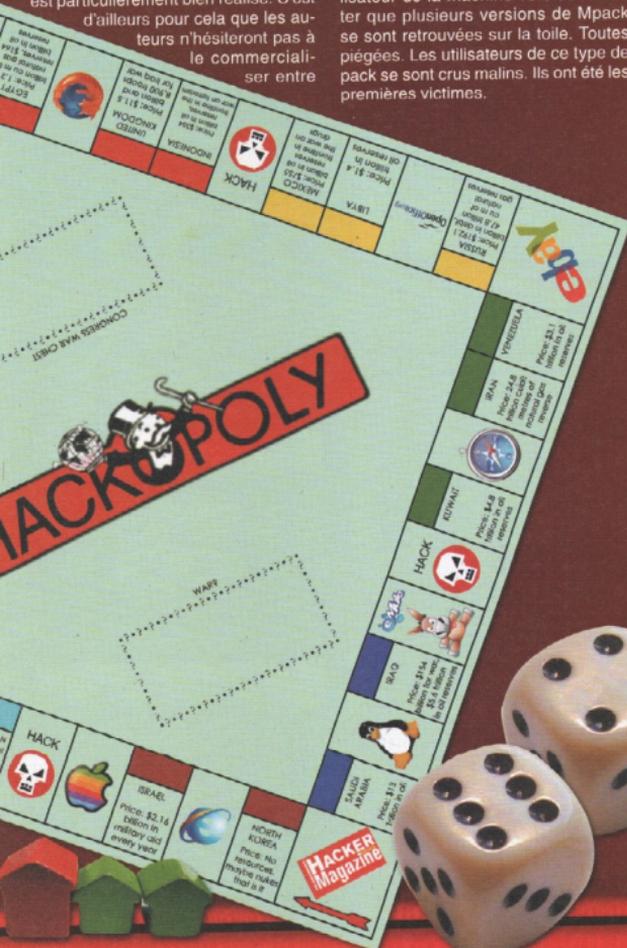
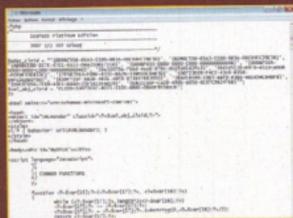
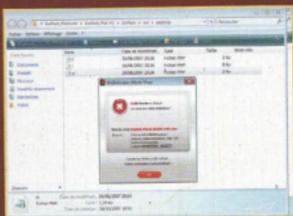


ble de pages en php capable d'exploiter plusieurs failles visant les navigateurs du marché (Internet Explorer, Firefox, Opéra, ...). Les sites italiens, comme des milliers d'autres se sont vus infiltrer. Objectif, insérer des balises html iFrames piégées afin de renvoyer sur des sites pirates qui hébergeaient Mpack. Les visiteurs des sites piégés ne se rendaient compte de rien. En toute transparence, et si leur navigateur n'avait pas été mis à jour il se retrouvait infecté et à la merci des pirates. Mpack est particulièrement bien réalisé. C'est d'ailleurs pour cela que les auteurs n'hésiteront pas à le commercialiser entre

400 et 700 dollars, selon les versions. Dans ce couteau Suisse du piratage, une base de données SQL avec différentes tables (maketable.php) qui permettent de générer des statistiques (Nombre de victimes, pays, ip des cibles, navigateurs, identifiant pour chaque machine piégées, ...). Une fois l'internaute piégé Mpack installe un cheval de Troie (Trojan) du nom de Torplg. Un outil espion qui n'a qu'une seule mission, voler les identifiants de connexion aux banques utilisées par l'utilisateur de la machine volée. A noter que plusieurs versions de Mpack se sont retrouvées sur la toile. Toutes piégées. Les utilisateurs de ce type de pack se sont crus malins. Ils ont été les premières victimes.

## :: IcePack, un Mpack venu du froid

Dans la lignée des Mpacks, IcePack est le grand frère numérique de ces couteaux Suisses. Commercialisés plusieurs centaines de dollars, des versions piratées et piégées ont été diffusées gratuitement la toile.

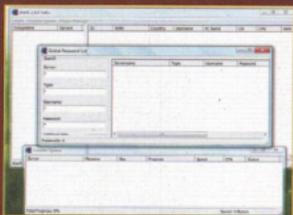


Apparu en août 2007, IcePack n'est rien d'autre que le frère de Mpack. Différence, le groupe IDT a tenté de brouiller les pistes de ces méfaits. Déjà, IcePack était, lui aussi, commercialisé. Mise à prix, 400 dollars. Toujours le même principe. Framework et mise à jour durant un an des exploits potentiels. Icepack optimise Mpack avec toujours le même principe de base de données et une

administration plus « claire » afin de suivre l'évolution des victimes. IcePack propose, entre autre, de diffuser une vidéo Quicktime compromise. Parfait, pour les pirates, pour injecter leur code malicieux dans la machine d'une victime. Les auteurs de Icepack doivent gagner pas mal d'argent avec ce type d'outil. Ils se sont « fatigués » à préparer pas moins de 200 serveurs contenant Icepack. Finesse ultime, comme pour Mpack, les auteurs de cette boîte à outil n'ont pas oublié de cacher une backdoor dans IcePack. Bilan, les utilisateurs se font eux même piégés. Aujourd'hui, plusieurs autres variantes sont apparues de cet outil pas comme les autres. La rumeur fait même état de son utilisation dans les dernières grosses attaques du moment, dont celle ayant visé, fin octobre, l'un des serveurs de la régie publicitaire 24/7 Real Media. Via cette infiltration, des bannières publicitaires ont été infectées par un code malicieux exploitant la fameuse vulnérabilité RealPlayer découverte par Symantec (voir nos news, NDR). Des pirates informatiques, après avoir gagnés l'accès au serveur de 24/7 Real Media, ont injectés une balise Iframe dans chaque publicités délivrées par le serveur. Un cheval de Troie était installé, une variante de Zonebac.

## :: Shark Project

Un nouveau cheval de Troie, un trojan, qui défraye la chronique depuis quelques semaines. Même si son auteur a stoppé le codage de Shark, les pirates l'utilisent et en abusent sans modération !

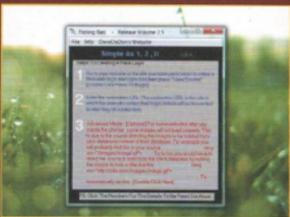


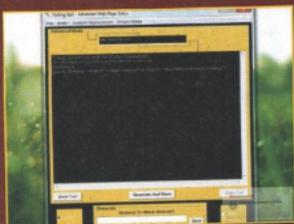
En septembre dernier apparaissant le Shark Projet. Un outil servant à créer des chevaux de Troie, des logiciels espions. Luis Corrons, de Panda.Labs indiquait « Ces chevaux de Troie représentent une menace pour la confidentialité des utilisateurs puisque les cybercriminels peuvent même activer la webcam de l'ordinateur et voir ce qu'ils font ». Seulement, après nos tests, nous avons découvert que Shark pouvait faire, malheureusement, bien plus que d'ouvrir un web cam. Avec la version 2 de Shark, les pirates peuvent spécifier le serveur auquel le cheval de Troie doit se connecter et programmer le malware pour qu'il s'exécute à chaque redémarrage du système, affiche des messages d'erreur ou exécute d'autres fichiers. Cet outil de piratage permet également d'effectuer d'autres actions malveillantes telles que stopper certains processus et services, intercepter le numéro de série de Windows, intercepter les comptes Stream, les mots de passe sauvegardés sous Internet Explorer, Firefox, créer des copies d'écran de l'ordinateur ciblé, captures audio et un keylogger qui permet d'enregistrer les frappes effectuées au clavier, interception

des mots de passe Outlook, FTP, Htaccess, accéder à la médiathèque, découvrir ce qui a été téléchargé sur le P2P, ... Quelques semaines après la diffusion de cet « outil », le créateur de ce trojan, « Niper109, un allemand, va décider de tout stopper. « Trop de personnes ont utilisé Shark à de mauvaises fin, confiait-il. L'idée de ce projet était de lancer un grand défi de codage ». Une fermeture qui est surtout la raison d'une nouvelle loi Allemande, la fameuse « loi anti-hacker » qui interdit à toute personne la création, la possession, la mise en service/distribution ou encore la publication de logiciel permettant des actions d'espionnage, de sabotage ou permettant la modification d'un système hardware ou software. Peur d'une forte amende ou d'emprisonnement. Certainement !

## :: Phishing Kit

Il n'y a jamais eu autant d'attaques phishing. Ces escroqueries à la fausse page bancaire évoluent, se professionnalisent. Avec l'arrivée d'outil de création d'attaque phishing, autant dire que les pirates n'ont pas fini de nager dans les eaux troubles du web.





Depuis quelques temps déjà, les kits phishing, des dossiers remplis de fausses pages de banques et autres boutiques en ligne se diffusent sur Internet, soit contre des poignets de dollars, soit gratuitement, mais avec des bonus pirates que les utilisateurs ne perçoivent pas toujours. Avec le logiciel Fishing-Bait, autant dire que le travail des pirates est mâché pour le moindre pousse bouton en mal d'escroquerie. Fishing-Bait est sous la forme d'un petit programme infor-

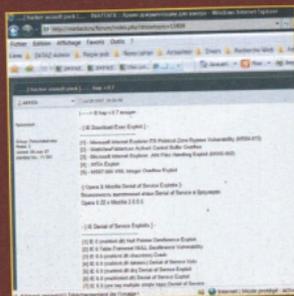
matique. Il ne pèse que 148 Ko. Son auteur indique que son «outil» n'est mis à disposition sur la toile qu'à but d'information. Une mission pourtant assez trouble, elle permet tout de même aux pirates de se créer une page phishing en quelques clics de souris. D'autant plus que l'auteur diffuse sur son forum des pages pirates prêtes à l'emploi, visant AOL/AIM, DailyMotion, EverQuest Forum, Facebook, FileFront, Gmail, Habbo, Hi5, MySpace, Photobucket, RapidShare, Ripway, Skype, VanGuard, Yahoo, YouTube, ... Fishing bait permet une automatisation totale. Il se charge de créer le script phishing. Le pirate n'a plus qu'à y installer la fausse page formulaire du site visé, une banque par exemple. L'escroc n'a plus qu'à cacher le tout sur un serveur qu'il aurait, soit piraté, soit loué à cette occasion. Autant dire qu'avec ce type de logiciel, le premier idiot du village venu pourra se lancer dans le phishing.

la famille Mpack et Icepack. Toujours la même facilité d'exploitation automatique de plusieurs exploits à partir d'Internet Explorer (IE ITS Protocol Zone Bypass Vulnerability MS04-013 ; WebViewFoldericon ActiveX Control Buffer Overflow ; IE .ANI Files Handling Exploit MS05-002 ; XHTA Exploit. Les autres navigateurs ne sont pas oubliés. Opéra et Firefox avec plusieurs possibilités de Déni de Service (DoS). Pour Internet Explorer de Microsoft (IE6 Sp2), dix-sept possibilités de DoS. Le pirate commercialisé cet outil sous trois forme, du «lite» au «pro».

Et que dire du piratage de l'ambassade des USA en Russie, victime, elle aussi, d'un autre pack, inconnu mais tout aussi efficace. Lors du Milipol 2007, en octobre dernier à Paris, a été présenté le Remote Control System. Un système d'espionnage informatique proposée par la société italienne « Hacking Team ». Du piratage éthique proposées par cette PME à destination d'États et Forces de l'ordre. « Notre produit est invisible aux antivirus et autres outils de protection » confiait l'un de commerciaux. Bref, vous l'aurez compris, mettez un pied devant l'autre sur la toile commence à devenir compliqué. Il est plus que conseillé de mettre à jour ses logiciels (OS, Navigateur, antivirus, ...) et de s'équiper d'une prudence à toute épreuve. ■

## COMMENT SE PROTÉGER ?

**S**imple et compliqué à la fois, les pirates usent de nouvelles méthodes d'infiltration. Pas une journée sans un exploit qui peut mettre à mal nos machines ou des sites Internet pourtant considéré comme «secure». Première évidence, afin de se sécuriser un maximum, mettre à jour ses outils comme ses navigateurs. Internet Explorer, Firefox, ... tous peuvent être exploités par des pirates. Mise à jour, aussi, de vos outils de protection : antivirus, firewall, ... Dernier point, arrêtez d'installer tout et n'importe quoi sur vos ordinateurs. Plus vous aurez de logiciels, plus vous aurez de chance de tomber face à une faille exploitant l'un de ces programmes. Il existe un grand nombre de logiciels gratuits de très bonne facture pour mettre en place une sécurité sérieuse sur votre machine, n'hésitez pas à les visiter : antivirus-enligne.com ; firewall-gratuit.com ; ...



## :: n404, Hacker Assault Pack and Co

Comme vous venez de le voir, les packs et autres outils «clé en main» ont pris le pouvoir sur la toile. Alors que ceux présentés sont plus ou moins public, il existe d'autres outils plus discret, plus confidentiel. Il aura fallu attendre le piratage de la Bank of India, fin août, pour découvrir les agissements du pack n404. Dans la même famille, le Hacker Assault Pack (HAP) signé d'un certain n0153r. La version 0.7 est sortie en septembre. HAP intègre une grande partie des options de

## DEFINITIONS D'UNE IFRAME

**L**e cabinet d'étude, XMCOPRTNERS a traduit l'attaque iFrame sous cette forme. Une iframe est une balise HTML permettant de regrouper plusieurs pages web en une seule. Elle permet donc à un pirate d'intégrer une page malicieuse au sein d'une page légitime. La taille de cette dernière est paramétrable (1 pixel) et peut donc paraître invisible à la vue des victimes.

Exemple

```
<iframe name="" SRC="http://www.
xxxx.com" scrolling="yes" height="1"
width="1" FRAMEBORDER="
yes"></iframe>
```

SCANDALE

# RÈGLE N°1 :

## Ne jamais voler un voleur !

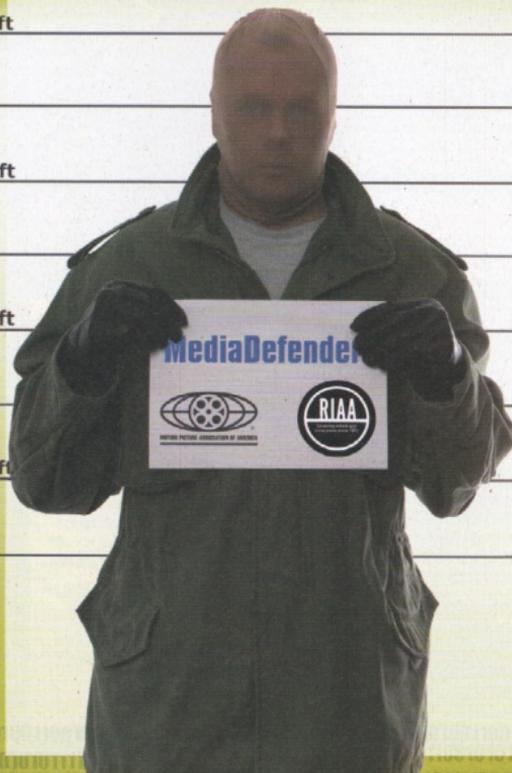
*Voici l'un des plus grands scandales de P2P de ce début de siècle !*

6 ft

5 ft

4 ft

3 ft



**Q**ue ses moyens d'action soient douteux, tout le monde le savait. Qu'elle ait tenté de saboter des serveurs et des sites, n'est plus un scoop. Mais ce que l'on a découvert ces derniers jours sur MediaDefender dépasse tout entendement.

Commençons par le début :

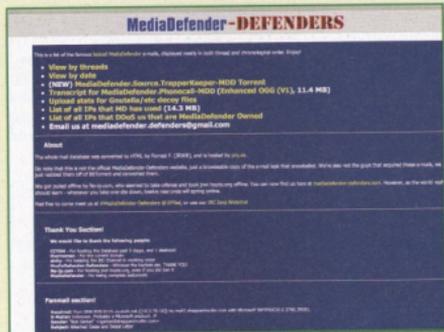
- MediaDefender.  
Mail: 200612.200709-MDD.3806944.  
TPB.torrent

Nous sommes autour du 15 septembre lorsque le fichier appelé MediaDefender.Mail.200612.200709 se met à circuler sur les plus gros sites torrents et ce, sans compter une certaine rumeur qui, elle aussi, se répand massivement : MediaDefender, la plus grande organisation d'antipiratage musical et cinématographique américaine - qui regroupe la RIAA (musique) et la MPAA (cinéma) - aurait "perdu" dans le réseau 700 Mo de courriels échangés entre les employés de la compagnie. Jusqu'ici, il y aurait de quoi rire mais à mesure que nous lisons les mails, le sourire prend vite des allures de grimace. Tout ce dont MediaDefender était accusée jusqu'à présent est confirmé par ces mails. On y trouve en effet toutes les tactiques, stratégies, adresses IP et commentaires du "bras armé" du front anti-P2P. Ces mails ont été échangés entre

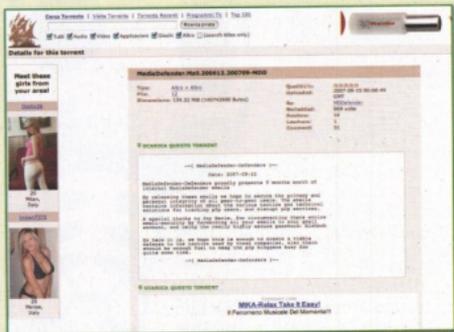
décembre 2006 et septembre 2007, et diffusés sur le Net par un groupe baptisé MediaDefender-Defenders qui n'a pas

hésité à revendiquer son acte en ces termes : "En diffusant ces e-mails, nous espérons garantir la pri-

vée et l'intégrité personnelle de tous les utilisateurs de peer-to-peer. Ces mails contiennent des informations



La véritable boîte de Pandore [www.media defender-defenders.com](http://www.media defender-defenders.com)



La page de ThePirateBay.org où télécharger le torrent des mails

sur les différentes tactiques et solutions techniques utilisées pour tracer les P2Pistes, et mettre sens dessus dessous les services de P2P".

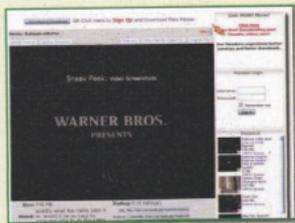
## :: Miivi.com et le reste

Autre scandale qui a frappé de plein fouet MediaDefender et confirmé par les mails : son site [www.miivi.com](http://www.miivi.com), utilisé ni plus ni moins pour piéger les utilisateurs en se faisant passer pour un site de P2P. Bref un véritable pot de miel qui invitait les P2Pistes à télécharger une application permettant d'accéder à un circuit de fichiers de partage : il s'agissait d'excellents contenus accompagnés de toutes dernières nouveautés cinématographiques.

Le hic ? Cette application recueillait des informations sur les utilisateurs et les envoyait ensuite à MediaDefender et à la MPAA. Mais le pot aux roses a vite été découvert. Un simple WHOIS sur le nom de domaine de Miivi.com a en effet permis de découvrir que MediaDefender en était l'heureux propriétaire. Après la fuite de données, le site est devenu inaccessible en moins de 24 heures. Le scandale a même fait descendre la MPAA sur le terrain, qui a désavoué, de façon un peu ridicule, MediaDefender. Pour sa part, la société s'est défendue en déclarant qu'il

s'agissait d'un projet interne qui (voyez-vous ça, comme c'est curieux !) aurait été publié on-line...

Il s'agirait en fait d'un "Appât", l'une des quatre techniques créées par MediaDefender et mises à disposition de ses clients qui, rappelons-le déboursent tout de même la modique somme de 5 000 à 15 000 dollars". Seconde technique utilisée ? Le "Spoofing", un système qui interagit avec les réseaux P2P : ceux qui recherchent du matériel reçoivent de faux résultats, afin de les décourager à poursuivre leurs recherches. Troisième technique ? L'"Interdiction" qui prévoit en revanche une approche différente, à savoir empêcher ceux qui diffusent des fichiers sur le Net, de jouer leur propre rôle. Il s'agit de saturer la bande passante d'upload du pirate avec des



Premier scandale, le site [miivi.com](http://miivi.com) de MediaDefender

centaines de fausses demandes, en réduisant ainsi ou en bloquant sa capacité de partage. Dernière technique ? Le "Swarming" : polluer un torrent BitTorrent avec un flux de fragments vides ou corrompus, comme l'a fait par le passé le célèbre réseau par câble HBO. Bien que le protocole soit en mesure d'écarter ces parties, le résultat final se traduit par une aggravation drastique des performances globales : le téléchargement du fichier en question est plus que lent. Bref, quel beau palmarès...

## :: Le jour suivant...

Tout ce que nous venons de vous raconter (et bien d'autres choses encore), est confirmé par le contenu de nos fameux mails "partagés". MediaDefender a également tenté de faire pression mais sans succès. Elle a en effet envoyé des sommations aux différents sites torrents



tente de nuire à ce site et aux nombreux bittorrents en général, ne peut s'attendre qu'à un grand \*\*\*\*\* de notre part..." et de poursuivre avec toute une série de conseils sur la façon d'aller se faire...

Enfin, The Pirate Bay a pris la balle au bond en décidant de porter plainte - comme il l'annonce sur son site - contre des majors d'Hollywood directement liés à MediaDefender : Twentieth Century Fox, Emi Music, Universal Music Group, Universal Pictures Nordic, Paramount Home Entertainment, Atari Nordic, Activision Nordic Filial Till Activision Ltd, Ubisoft Sweden, Sony Bmg Music Entertainment et Sony Pictures Home Entertainment Nordic.

Les accusations sont graves et se basent justement sur les éléments relevés dans le paquet d'e-mails : sabotage d'infrastructures, déni de service, cracking et spamming. En outre, cette plainte n'a pas été déposée à titre personnel mais en tant que société. Les éventuelles amendes n'en seront que plus onéreuses. Pour célébrer cette plainte, nos amis de la Baie ont également lancé une nouvelle page d'accueil.



## Des mails et bien plus...

Face à toute cette cohue, il faut également ajouter d'autres découvertes démasquant MediaDefender : plusieurs appels téléphoniques, toujours traçables sur les sites torrents, viennent en effet confirmer le contenu des mails. Et, chose plus intéressante,

le code source du software qui était téléchargé sur mivi.com, a également été diffusé sur le réseau par mediadefender-defenders.com, accompagné de la revendication suivante : «Les MediaDefender-Defenders sont heureux de vous présenter

le code source utilisé par MediaDefender. Ce code est complet et concerne toutes les opérations réalisées sur KaaZaa, BitTorrent, Gnutella [...]. Nous dévoilons ces informations au public pour que l'on puisse identifier les types d'appâts utilisés par MediaDefender. Nous remercions tout particulièrement les employés de MD qui nous ont fourni le matériel». Que dire, si ce n'est que ces P2Pistes sont également très spirituels !

Titre	Nomme
Altre > Altre	MediaDefender Source.TrapperKeeper-MDD
Altre > Altre	MediaDefender.Photovall-MDD
Altre > Altre	MediaDefender.Pail.200261.200792-MDD

Voici les autres fichiers tout droit "sortis" de MediaDefender et prêts à finir sur les PC du monde entier

## Conclusion

Difficile de tirer des conclusions sur toute cette histoire surtout lorsqu'on sait qu'elle est loin d'être finie. D'autres données seront extraites du matériel tout droit sorti de MediaDefender. Nous ignorons si tout cela conduira à une tentative de réconciliation entre

les majors et sites de partage de fichiers ou encore à un nouveau durcissement de la lutte déjà engagée. L'action de The Pirate Bay ferait plutôt penser au déclenchement d'une guerre sans pitié. Et nous ne sommes sans doute pas les seuls à le penser. MediaDefender s'est donc laissé prendre à son propre jeu, en écrivant ainsi la fin de son histoire. Mais nous sommes sûrs qu'une autre entité jaillira de ses cendres toujours dans le but d'arrêter la diffusion du P2P. En effet, nous ne croyons pas que la RJAA et la MPAA soient disposées à céder sur ce point, mais sans doute seront-elles à présent plus attentives quant aux méthodes adoptées. Qui vivra verra !!!



La page d'accueil dédiée à la plainte de la Baie contre les majors

# JUILLET

1	M	
2	M	
3	J	
4	V	
5	S	
6	D	
7	L	
8	M	
9	M	
10	J	
11	V	
12	S	
13	D	
14	L	
15	M	
16	M	
17	J	
18	V	
19	S	
20	D	
21	L	
22	M	
23	M	
24	J	
25	V	
26	S	
27	D	
28	L	
29	M	
30	M	
31	J	

# AOÛT

1	V	
2	S	
3	D	
4	L	
5	M	
6	M	
7	J	
8	V	
9	S	
10	D	
11	L	
12	M	
13	M	
14	J	
15	V	
16	S	
17	D	
18	L	
19	M	
20	M	
21	J	
22	V	
23	S	
24	D	
25	L	
26	M	
27	M	
28	J	
29	V	
30	S	
31	D	

# SEPTEMBRE

1	L	
2	M	
3	M	
4	J	
5	V	
6	S	
7	D	
8	L	
9	M	
10	M	
11	J	
12	V	
13	S	
14	D	
15	L	
16	M	
17	M	
18	J	
19	V	
20	S	
21	D	
22	L	
23	M	
24	M	
25	J	
26	V	
27	S	
28	D	
29	L	
30	M	



# AVRIL

1	M
2	M
3	J
4	V
5	S
6	D
7	L
8	M
9	M
10	J
11	V
12	S
13	D
14	L
15	M
16	M
17	J
18	V
19	S
20	D
21	L
22	M
23	M
24	J
25	V
26	S
27	D
28	L
29	M
30	M

# MAI

1	J
2	V
3	S
4	D
5	L
6	M
7	M
8	J
9	V
10	S
11	D
12	L
13	M
14	M
15	J
16	V
17	S
18	D
19	L
20	M
21	M
22	J
23	V
24	S
25	D
26	L
27	M
28	M
29	J
30	V
31	S

# JUIN

1	D
2	L
3	M
4	M
5	J
6	V
7	S
8	D
9	L
10	M
11	M
12	J
13	V
14	S
15	D
16	L
17	M
18	M
19	J
20	V
21	S
22	D
23	L
24	M
25	M
26	J
27	V
28	S
29	D
30	L

# OCTOBRE

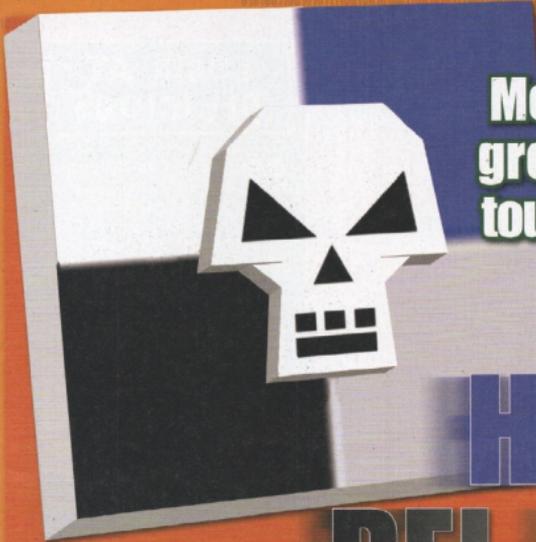
1	M	
2	J	
3	V	
4	S	
5	D	
6	L	
7	M	
8	M	
9	J	
10	V	
11	S	
12	D	
13	L	
14	M	
15	M	
16	J	
17	V	
18	S	
19	D	
20	L	
21	M	
22	M	
23	J	
24	V	
25	S	
26	D	
27	L	
28	M	
29	M	
30	J	
31	V	

# NOVEMBRE

1	S	
2	D	
3	L	
4	M	
5	M	
6	J	
7	V	
8	S	
9	D	
10	L	
11	M	
12	M	
13	J	
14	V	
15	S	
16	D	
17	L	
18	M	
19	M	
20	J	
21	V	
22	S	
23	D	
24	L	
25	M	
26	M	
27	J	
28	V	
29	S	
30	D	

# DÉCEMBRE

1	L	
2	M	
3	M	
4	J	
5	V	
6	S	
7	D	
8	L	
9	M	
10	M	
11	J	
12	V	
13	S	
14	D	
15	L	
16	M	
17	M	
18	J	
19	V	
20	S	
21	D	
22	L	
23	M	
24	M	
25	J	
26	V	
27	S	
28	D	
29	L	
30	M	
31	M	



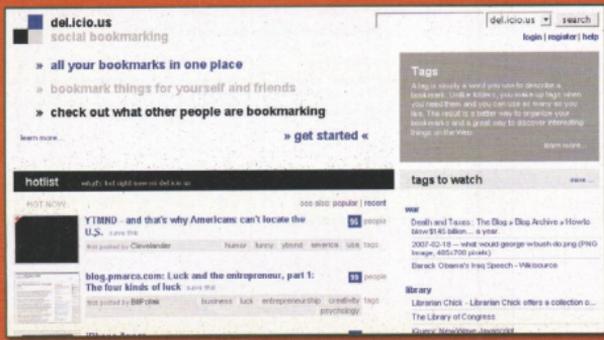
**Menaces sur le plus gros site américain : toutes les révélations en exclu !**

# HACKING DEL.ICIO.US

*Voici quelques trucs pour utiliser "autrement" le service de bookmarking online et le rendre encore plus personnel et indispensable*

En ligne depuis 2003, del.icio.us est l'un des vétérans du Web 2.0, et sans doute celui qui est resté le plus fidèle à l'idée d'origine de son créateur, Joshua Schachter, malgré son rachat par Yahoo!

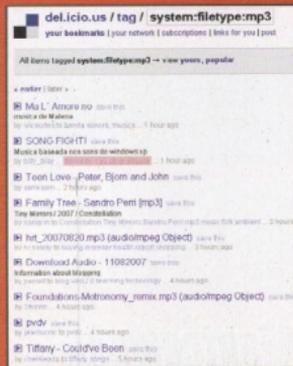
L'objectif est aujourd'hui de vous aider à organiser vos informations. Del.icio.us se présente donc officiellement comme un outil online pour organiser vos bookmarks. Mais derrière une façade épurée, se cachent de nombreuses caractéristiques et un grand potentiel peu connu, qui n'attendent qu'une chose : être exploités !



## :: Musique, bookmarks !

Del.icio.us n'est pas seulement un outil. C'est aussi une ressource pour de nouvelles idées, lectures et... autres.

Parmi les tags prévus, on trouve un tag système inséré automatiquement, que peu de gens connaissent : `system:filetype:mp3`. En lançant une recherche avec ce tag spécial, vous aurez accès à toute la musique dénichée ici et là par les autres utilisateurs sur <http://del.icio.us/tag/system.filetype:mp3>



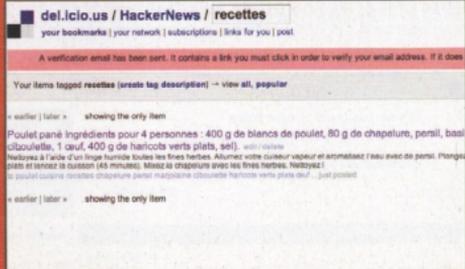
On y trouve un peu de tout : des podcast aux morceaux commerciaux en passant par des remix, mashup ou cover

(comme le thème de Super Mario Bros, revu par le London Symphony Orchestra). Si vous voulez uniquement accéder aux quelques fichiers audio les plus écoutés (ajoutés aux bookmarks) par les utilisateurs, rendez-vous sans attendre sur <http://del.icio.us/popular/system:filetype:mp3>. Vous pouvez y télécharger les fichiers ou les écouter via votre navigateur, grâce à un lecteur en Javascript déjà incorporé dans les pages de del.icio.us.

## :: Repas vraiment del.icio.us !

Chaque entrée de del.icio.us se compose de quatre champs : url, description, notes et tags. Les champs Description et notes sont prévus pour accueillir le titre et les commentaires d'un url. Rares sont ceux qui savent que leur capacité atteint 255 caractères. Ce qui suffit largement pour un post sur un blog (que l'on synchronisera avec son propre site) ou pour tout type d'annotation, même des recettes de cuisine !

Impossible ? Au contraire : si vous allez sur <http://del.icio.us/HackerNews/recettes> vous verrez qu'avec un peu d'inventivité et de discipline, del.icio.us peut se transformer en un véritable coffre à recettes pour épater et conseiller ses amis. Pour ajouter une recette, on crée un nouveau bookmark (via bookmarklet ou à l'adresse <http://del.icio.us/post>). L'adresse n'a pas une grande importance en soi : vous pouvez taper une fausse adresse ou encore une adresse erronée, l'essentiel étant qu'elle existe et qu'elle soit unique. Le titre doit contenir le nom de la préparation mais aussi toutes ces informations générales, comme le nombre de personnes prévues pour ce plat, la difficulté de préparation, le temps nécessaire... Le véritable défi tient ici à la description et vous disposez des 255 caractères pour faire entrer tant les ingrédients et leur poids que la recette à proprement dit. Enfin, vous trouverez



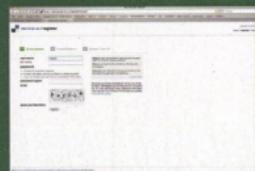
le champ des tags, indispensable pour vous rappeler de ce dont vous avez besoin, qu'il s'agisse du type de plat (entrée, pâtes, sauce), de l'origine (Italie, Méditerranée), des ingrédients (pâtes,

## LOGIN AT DEL.ICIO.US

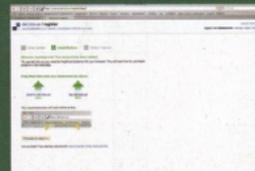
Pour ceux qui n'auraient jamais eu affaire à ce service, voici quelques infos sur son utilisation. Vous trouverez le site de référence sur <http://del.icio.us>. Vous pouvez l'enregistrer à partir de la home page en cliquant sur "get started".



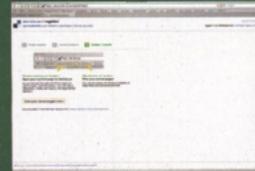
Vous devez à présent entrer vos données :



et les liens seront directement mis à disposition vers votre page et la page d'accueil de del.icio.us.



Dès lors, votre page est active.





## DE DELICIOUS AU BLOG

**D**el.icio.us peut aussi être utilisé pour insérer de brefs commentaires et textes (jusqu'à 255 caractères) sans avoir à entrer dans l'interface d'administration de son propre blog ou site web basé sur Wordpress. Une opération rendue possible grâce au script en php "yadd: yet another daily delicious" (<http://www.clampcampus.com/plugins/yadd.txt>) de Marc Nozell ([www.nozell.com/blog/](http://www.nozell.com/blog/)). Installé sur son propre serveur, lorsqu'il est activé, il récupère à partir de del.icio.us les bookmarks ajoutés dans la journée et les publie comme entrée de Wordpress.

des autocollants Pantone si chers aux graphistes et qui aujourd'hui est à la portée des webdesigners. Le tag facultatif, mais souvent utilisé sur del.icio.us pour ces favoris pour le moins spéciaux, n'est autre que "ColorScheme". Vous pouvez voir les palettes des autres utilisateurs sur <http://del.icio.us/tag/ColorScheme>. Vous pouvez bien évidemment les copier comme n'importe quelle autre adresse grâce à la fonction-link "save this". Vous découvrirez par là même la syntaxe "color:hex,hex" qui permet d'indiquer les couleurs.

Par exemple, la combinaison suivante dans le champ "url"

```
color:8dbfe0,bee183,f2b2cd,dadbdd,ddc891
```

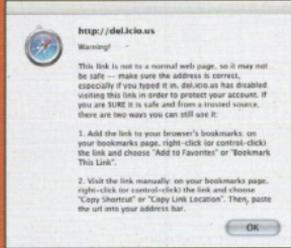
se retrouve dans la palette de couleurs des iPod d'Apple, tandis que cette séquence

```
color:85C229,3BAE01,D10202,000099
```

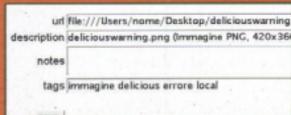
est en revanche la palette de base des pages web de Technorati.

Les séquences hexadécimales doivent être composées de six caractères. Elles peuvent être réalisées avec des logiciels ou ressources comme Kuler d'Adobe ou encore prélevées de la source de n'importe quel site web à l'aide d'un simple copier/coller.

fonctionne pas - sur certains navigateurs, par précaution, le système n'insère pas le bookmark - il suffit de faire un copier/col-



ler de l'adresse dans le navigateur du fichier et de la coller dans le champ 'url' d'un nouveau bookmark. Et pour ceux qui



s'inquiètent déjà quant au respect de leur confidentialité, ajoutons que tous les bookmarks de fichiers locaux sont automatiquement enregistrés comme "privés", et sont visibles et récupérables uniquement par leur propriétaire légitime.

Nicola D'Agostino

## :: Un peu de couleurs

Mais il existe aussi d'autres utilisations de del.icio.us ne nécessitant aucune adresse web, comme par exemple l'archivage des couleurs.



Le champ url permet d'indiquer des palettes de couleurs en utilisant la syntaxe hexadécimale du HTML et des CSS, que le serveur affichera ensuite dans la liste des bookmarks sous forme de "chip", de petits rectangles colorés, sur l'exemple

## :: Bookmarks locaux

Enfin, pour les inconditionnels de la formule d'archivage de del.icio.us, il existe un moyen de l'étendre au contenu sur son propre ordinateur. Les bookmarks et les tags peuvent aussi cibler des fichiers en local. Il suffit d'utiliser la bonne syntaxe qui, sur Windows, donne : fichier:///lettredisque//parcours/fichier.doc. Sur Unix/Linux, cela donnera fichier:///parcours/nom/fichier.odt. Enfin, sur Mac, cela devrait donner quelque chose comme fichier:///parcours/fichier.txt. Pour ajouter l'url d'un fichier local, la façon la plus rapide consiste à le faire glisser dans le navigateur pour utiliser ensuite le bookmarklet fourni par le service - si vous utilisez Firefox - grâce au bouton "tag" de l'extension del.icio.us de Yahoo! <https://addons.mozilla.org/fr/firefox/addon/3615>. Si cela ne

## CONTESTATION

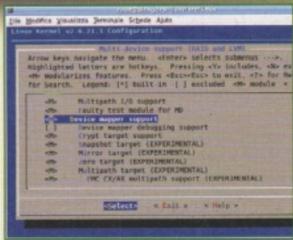
**A**vez-vous déjà vu un bookmark qui cible aucun site mais qui contient des informations aussi précieuses qu'interditées ? C'est arrivé en mai, tandis que la protection AAC3 a été percée pour la première fois. Del.icio.us était aussi présent parmi le florilège d'initiatives qui ont diffusé et décliné online les codes pour déprotéger les DVD. Ici, la séquence incriminée qui commence par 09F9 a été archivée et trône encore en toute tranquillité sous forme d'une simple palette de couleurs.

Découvrez comment protéger le contenu d'une clé USB ou d'un DVD face aux regards indiscrets !

# La clé invisible

**C**acher ses données personnelles n'est parfois qu'une simple mesure de précaution, mais peut devenir très vite une nécessité pour certains. Si vous avez pour habitude d'utiliser des clés USB et des DVD pour enregistrer des informations qui doivent absolument rester confidentielles, vous pouvez alors les confier à un algorithme de cryptage infailible : quelles que soient les mains dans lesquelles elles tomberont, vos informations seront illisibles !

Commençons par le cryptage d'une clé USB. Tout d'abord, assurez-vous que votre kernel (noyau) dispose bien du support pour le device mapper (mappeur de périphériques) et dm-crypt : dans la configuration du kernel, entrez dans Device Drivers > Multi-device support et assurez-vous que les rubriques "Device mapper support" et "Crypt target support" soient sélectionnées. Enfin, dans la section



➊ Les modules à activer dans le kernel pour lancer les fonctions de cryptage des périphériques.

"Cryptographic options", activez l'algorithme de cryptage AES.

## Comment gérer les périphériques cryptés ?

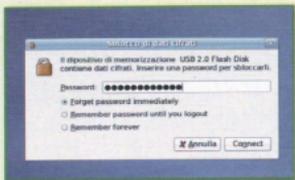
A présent, installez cryptsetup, le

programme pour manipuler des périphériques cryptés. Allez sur <http://luks.endorphin.org/dm-crypt>, téléchargez le pack `cryptsetup-1.0.5.tar.bz2` et décompressez-le avec "tar xvjf cryptsetup-1.0.5.tar.bz2". La compilation et l'installation s'effectuent comme d'habitude à travers la suite de commandes "configure, make, make install".

A présent, vous pouvez brancher votre clé USB sur votre PC. Localisez le fichier de périphérique correspondant à la clé, en lançant dans une console "dmesg" : une ligne d'output semblable à celle-ci "sd 4:0:0:0: Attached scsi removable disk sdb" vous indiquera le device approprié (/dev/sdb, dans l'exemple). Vous allez maintenant crypter la première partition présente sur la clé, /dev/sdb1. Initialisez la partition avec la commande suivante (par souci de simplicité, toutes les commandes présentes sont supposées être exécutées à partir du root) : `cryptsetup luksFormat /dev/sdb1`. Tapez "YES" pour confirmer l'opé-

ration, puis tapez deux fois (la seconde pour vérification) votre "passphrase" : il s'agit d'un mot de passe très long qui vous permettra d'accéder en clair au contenu de la partition, une fois que celle-ci aura été cryptée avec l'algorithme choisi (AES, par défaut). Une fois cette opération effectuée, ouvrez la partition cryptée de façon à créer un filesystem à l'intérieur : lancez "cryptsetup luksOpen /dev/sdb1 crypto" et tapez votre passphrase. Dès lors, vous avez un nouveau fichier de périphérique, qui permet d'accéder à la partition avec les données en clair : /dev/mapper/crypto. Vous vous servirez justement de ce nouveau device pour le formatage de la partition, en utilisant l'ancien filesystem Ext2 très fiable. Formatez avec "mkfs.ext2 /dev/mapper/crypto" et, à la fin de l'opération, fermez le device "crypto" en exécutant "cryptsetup luksClose crypto".

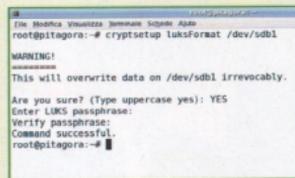
/dev/mapper/crypto /mnt/clé" (le répertoire /mnt/clé doit exister). Enfin, pour démonter le périphérique, tapez "umount /mnt/clé" et fermez le device crypté par le biais de "cryptsetup luksClose /dev/mapper/crypto". Remarque : vous pouvez également accéder à un périphérique crypté avec cryptsetup depuis Windows, en installant FreeOTFE (<http://www.freeotfe.org>).



**4** Vous utilisez Gnome ? Votre clé USB cryptée sera reconnue en tant que telle, automatiquement !



**4** Avec FreeOTFE, vous pouvez accéder à un périphérique crypté sous Linux même à partir de Windows...



**4** Pour initialiser la partition cryptée, vous devez taper une passphrase

## :: Entrez les données dans la clé cryptée

A présent, retirez la clé du PC et réinsérez-la. Si vous utilisez le bureau Gnome, alors préparez-vous à une agréable surprise : après avoir inséré votre clé, une fenêtre apparaîtra au milieu de l'écran, en vous demandant de taper votre passphrase pour déverrouiller le périphérique. Une fois cette passphrase entrée, vous aurez accès au contenu en clair de la clé depuis une fenêtre du gestionnaire de fichiers. Si vous n'utilisez pas Gnome, pour monter la clé USB, ouvrez le périphérique crypté avec "cryptsetup luksOpen /dev/sdb1 crypto", tapez votre passphrase, puis effectuez le montage du périphérique correspondant en clair par le biais de la commande "mount

DVD Filesystems > UDF file system support), présent dans les noyaux, à partir de la version 2.6.10.

Puis, préformatez votre support réinscriptible avec "dvd+rw-format -force /dev/dvd" (/dev/dvd est le fichier de périphérique pour le graveur de DVD), activez le Packet Writing en lançant "pktsetup 0 /dev/dvd", et initialisez le périphérique pour le chiffrement avec "cryptsetup luksFormat /dev/pktdvd/0".

Dès lors, ouvrez le périphérique crypté par le biais de "cryptsetup luksOpen /dev/pktdvd/0 pwdvd" (pwdvd est le fichier qui permet d'accéder en clair au contenu du DVD), créez un filesystem UDF à travers "mkudffs /dev/mapper/pwdvd" et, enfin, montez le DVD avec "mount -t udf /dev/mapper/pwdvd /mnt/pwdvd" (le répertoire /mnt/pwdvd, doit bien sûr exister). Copiez dans le répertoire /mnt/pwdvd tous les fichiers que vous souhaitez voir apparaître sur le DVD crypté. Une fois cette opération effectuée, démontez le DVD ("umount /mnt/pwdvd") et fermez le device en clair "pwdvd" avec "cryptsetup luksClose pwdvd". Voilà, c'est fini !

Pour accéder à votre DVD chiffré, il vous suffira d'activer le Packet Writing ("pktsetup 0 /dev/dvd"), d'ouvrir le périphérique crypté ("cryptsetup luksOpen /dev/pktdvd/0 pwdvd") et de le monter ("mount -t udf /dev/mapper/dvd /mnt/pwdvd"). Après avoir lu ou ajouté des données à partir du support, exécutez "umount /mnt/pwdvd" puis "cryptsetup luksClose pwdvd", avant de l'éjecter. ■



**4** Les opérations à effectuer dans la console pour lire votre DVD crypté.

## :: DVD crypté fonctionnant comme une clé USB

Passons à présent au chiffrement d'un DVD de données. Pour faciliter les opérations d'écriture, nous utiliserons la technologie Packet Writing : vous pourrez ainsi ajouter au fur et à mesure de nouvelles données lors des différentes sessions d'écriture, comme pour les clés USB. Tout d'abord, téléchargez le pack udfutils sur <http://sourceforge.net/projects/linux-udf> et installez-le à travers la traditionnelle séquence ".,configure, make, make install". Concernant le kernel, vous avez besoin du support aussi bien pour le Packet Writing (Device Drivers > Block devices > Packet writing dans la configuration) que pour l'UDF (File systems > CD-ROM/

# eMule Plus *L'autre visage de la mule*

*L'Open Source, c'est aussi ça : une version alternative qui parfois, fonctionne mieux que l'original !*

**M**ême si le circuit eDonkey est devenu l'un des réseaux de peer-to-peer les plus connus et utilisés au monde, grâce justement au programme du même nom, le programme de partage le plus utilisé n'est autre qu'eMule. Comme c'est souvent le cas dans le monde des programmes "ouverts", le célèbre mulet a lui

aussi fait l'objet de variations à n'en plus finir. Des variations que l'on appelle dans le jargon "modifications" ou, plus brièvement, "mod". On trouve des mods pour tous les goûts et toutes les exigences, plus ou moins fonctionnelles et efficaces, avec des variations plus ou moins profondes par rapport à l'original. Parmi toutes



## LE RISQUE

**C**omme c'est souvent le cas malheureusement en réseau, et plus particulièrement dans le cas du peer-to-peer, certains cherchent toujours à profiter de la bonne foi des utilisateurs. Si l'on cherche "emule plus" avec Google, l'un des premiers résultats donnés nous amène à l'adresse [www.emule.com](http://www.emule.com). La version d'eMule Plus, que l'on peut télécharger à partir d'ici, vous oblige à téléphoner à un numéro (899) pour obtenir un code d'installation pour le moins fantomatique, moyennant 3,00 €. Sachez que la version

qui sera installée est absolument identique à celle que vous pouvez télécharger sur le site officiel, où le programme d'installation a tout simplement été remplacé. Inutile de souligner le côté pernicieux de ce système, qui ressemble ni plus ni moins à une véritable escroquerie. Ceci dit, si vous voulez prendre à leur propre jeu ceux qui ont mis sur pied ce petit tour, le truc est simple : il suffit en effet d'insérer six caractères quelconques pour poursuivre l'installation !

celles existantes, eMule Plus est sans doute celle qui a remporté le plus grand succès parmi ses utilisateurs.

## :: Réseaux sélectionnés

Les spécificités qui caractérisent eMule Plus sont plutôt rares, mais restent néanmoins significatives.



## OÙ LE TROUVER ?

La page d'accueil officielle du projet eMule Plus se trouve sur <http://lemuleplus.info>. Là, vous aurez toujours accès à la toute dernière version, sans oublier un guide détaillé d'utilisation et la description de tous les différents composants du programme. Toujours sur le même site, vous pouvez consulter la liste des caractéristiques demandées par les utilisateurs pour les futures versions d'eMule Plus. Si vous avez un peu de mal avec l'anglais, il existe une page d'accueil officielle en italien. L'adresse dans ce cas est [www.emule.com/pt/emule-plus-1-2a.php](http://www.emule.com/pt/emule-plus-1-2a.php). La visite est recommandée surtout si vous n'êtes pas encore très familiarisés avec le "mulet". Vous disposez aussi section très complète appelée "Tips and tricks" où vous trouverez de nombreux conseils d'utilisation pour bien commencer et exploiter au mieux tout le potentiel du programme.



La première, absolument fondamentale, concerne la suppression du support du réseau 'décentré' Kademlia. L'utilité ou non de ce réseau alternatif continue aujourd'hui encore à faire couler beaucoup d'encre : bon nombre de personnes vantent ses mérites, l'autre moitié soulignant son inutilité. Quoi qu'il en soit, les programmeurs d'eMule Plus ont décidé de s'en passer. De nombreuses autres différences concernent la conception de l'interface. Celle-ci conserve bien sûr l'affichage général du programme, mais par rapport à eMule, cette version s'avère plus pratique et plus esthétique, ce qui n'est pas pour déplaire. La fenêtre principale regroupe en effet le plus d'informations possible, et prévoit même un panneau consacré aux détails du fichier sélectionné. Un

soin du détail très poussé, à tel point que le panneau de configuration a lui aussi été revu pour une plus grande simplicité d'utilisation. Si vous voulez contrôler le travail de votre mulet, même à distance, sachez qu'eMule Plus

a été le premier à utiliser une interface Web qui vous permet de gérer vos téléchargements même lorsque vous ne pouvez pas être physiquement devant votre ordinateur : il suffit pour cela de disposer d'une connexion Internet et d'un navigateur quelconque, et le tour est joué ! Autre possibilité : si vous avez un téléphone portable équipé de la technologie Java, vous pouvez même l'exploiter pour gérer vos téléchargements !

### :: Facile à utiliser

D'autres variations significatives ont été apportées dans tous ces domaines où l'on

pouvait améliorer la simplicité d'utilisation et la flexibilité du programme en général. Le panneau de recherches, par exemple, est sensiblement différent et vous permet de

## ACCÈS DISTANT

Pour activer le serveur Web d'eMule Plus, il suffit de cliquer sur le bouton **Préférences** dans la barre d'outils principale et de sélectionner la rubrique **Web Server** à la section **Connexion**. Cochez la case **Activé** et tapez le mot de passe souhaité. Vous pouvez laisser le port par défaut, sans oublier toutefois que vous devez l'ouvrir sur le firewall ou sur le routeur, si vous en avez un. La section **Hôte** vous permet de spécifier un autre utilisateur (avec un autre mot de passe) qui pourra accéder uniquement en consultation.



## LA FENÊTRE PRINCIPALE D'EMULE PLUS

### BOUTONS FONDAMENTAUX

La barre d'outils principale contient les boutons habituels pour accéder aux différentes sections du programme. En cliquant avec le bouton droit et en sélectionnant "Personnaliser", vous pouvez choisir les boutons à afficher et leur position. Toujours avec le bouton droit, vous pouvez appliquer une skin ou souligner les étiquettes de texte.

### PANNEAU

Chaque panneau de l'interface principale contient, à gauche du bouton du nom, une petite icône en forme de triangle. En cliquant dessus, vous pourrez le "fermer" temporairement, de façon à laisser plus d'espace aux panneaux restants. Pour ouvrir le panneau, il suffit bien évidemment de cliquer de nouveau sur l'icône.

### FICHER EN SORTIE

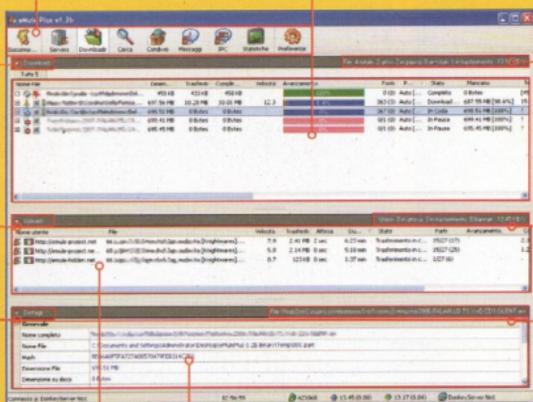
Juste en dessous, vous trouverez le panneau "Uploads", contenant la liste des fichiers que d'autres utilisateurs téléchargent actuellement sur vous. Ici aussi, vous avez deux icônes qui représentent le client utilisé par l'utilisateur (eMule ou autre) et sa nationalité.

### FICHIERS EN ATTENTE

Le panneau "Downloads" liste les fichiers que vous êtes en train de télécharger. À gauche du nom de chaque fichier, sont présentes trois petites icônes qui indiquent respectivement l'état (download, pause, complété etc.), le type de fichier et la présence de commentaires.

### SITUATION

La partie droite de la barre de titre des trois panneaux contient d'autres informations. Dans le cas des Downloads, vous verrez s'afficher le nombre de fichiers totaux, actifs et en pause, outre la vitesse actuelle de téléchargement. Pour les uploads, vous trouverez en revanche le nombre d'utilisateurs en attente et en transfert, plus la bande utilisée. Pour le panneau détails, vous obtiendrez le nom du fichier ou de l'utilisateur sélectionné.



### DETAILS

Le panneau Détails contient une description des éléments sélectionnés dans l'un des deux panneaux supérieurs. Si vous cliquez sur un fichier, vous verrez s'afficher tous les détails concernant sa taille, son type, ses sources, l'état du téléchargement et ainsi de suite ; si en revanche vous sélectionnez un utilisateur, vous aurez des informations sur son pseudo, le programme qu'il utilise, le serveur auquel il est connecté et bien d'autres choses encore.

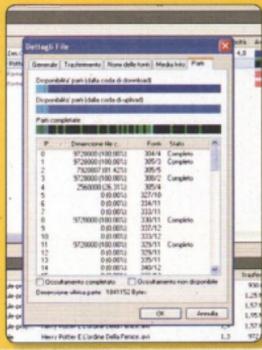
chercher les fichiers de façon plus ciblée, en spécifiant plusieurs filtres par rapport aux possibilités offertes par eMule. Si dans la dernière version vous pouviez en effet indiquer uniquement le nom et la catégorie du fichier à chercher (archive,

**► eMule Plus inclut un petit serveur Web qui permet de suivre les téléchargements même quand vous n'êtes pas devant votre ordinateur.**



## INFOS A GOGO

Nous avons déjà souligné à plusieurs reprises qu'eMule Plus avait fait de la simplicité d'utilisation l'un de ses chevaux de bataille. En cliquant sur l'icône du type de fichier à côté du nom, vous ouvrirez une fenêtre contenant une quantité incroyable de détails concernant le fichier sélectionné. Les différents onglets de la fenêtre informations vous permettent d'afficher toutes les caractéristiques du transfert (sources, nombre de parties totales et disponibles, taux de transfert), les noms attribués par les différents utilisateurs au fichier (utile pour le renommer rapidement sans avoir à retaper son nom), les détails relatifs aux caractéristiques des fichiers multimédia (taille de la fenêtre vidéo, type de codec utilisé, nombre de canaux audio, bitrate etc.) et même un récapitulatif très complet des parties disponibles.



peuvent tout de même être informés de l'avancement des opérations de téléchargement : eMule Plus possède en effet une option qui permet d'envoyer automatiquement un e-mail chaque fois qu'un fichier a été téléchargé. On trouve aussi toute une série de trucs moins évidents, dans la mesure où ils sont cachés dans les options de configuration. Combien de fois avez-vous perdu un téléchargement, peut-être lancé depuis plusieurs jours, à cause d'une simple coupure de courant ou d'un bug de Windows ? Grâce à la possibilité de forcer la création d'une copie de sauvegarde des fichiers temporaires et fichiers de configuration, vous pourrez conjurer le sort une bonne fois pour toutes ! En outre, eMule Plus peut aussi faire une copie de la liste des liens en attente. Ainsi, si par exemple un des fichiers que vous avez téléchargé est endommagé (cas rare mais pas improbable), vous pourrez immédiatement recommencer le

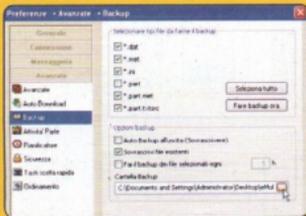


téléchargement sans avoir à effectuer de nouvelle recherche ou récupérer le lien. Bref, si vous n'êtes toujours pas convaincus de la qualité d'eMule Plus, il ne vous reste plus qu'à le mettre à l'essai ! Comme toutes les versions modifiées du client, la version Plus est 100% compatible avec les fichiers temporaires d'eMule "standard", c'est pourquoi vous pouvez tranquillement

l'installer et utiliser le même dossier que les fichiers temporaires de votre mulet chéri, en prenant soin, si vraiment vous ne souhaitez courir aucun risque, de faire une copie de sauvegarde des fichiers contenus dans le dossier. La seule précaution à prendre, si l'on veut avoir la possibilité de réutiliser la version normale, c'est de choisir un dossier d'installation différent de celui par défaut, de façon à ne pas écraser les fichiers d'eMule avec ceux de la version Plus. ■

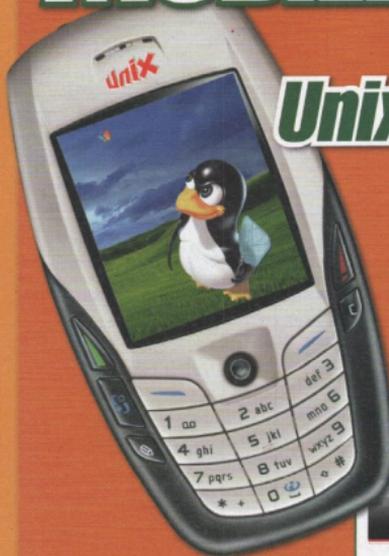
## ACTIVER LE BACKUP

Ceux qui ont pour habitude d'utiliser le mulet ont déjà dû perdre un ou plusieurs téléchargements à cause d'un bug du système ou d'une coupure de courant. Si vous voulez vous protéger définitivement contre tout risque de ce genre, vous pouvez effectuer automatiquement un backup des fichiers critiques. Cliquez sur Préférences, sélectionnez la section Avancés et cliquez sur Backup. En cochant les différentes cases, vous pouvez décider des types de fichier dont vous souhaitez faire une copie de sauvegarde (par exemple les fichiers ".ini" de configuration ou les ".met" qui contiennent les informations sur les différents blocs téléchargés). Mais n'oubliez pas que si vous sélectionnez aussi les fichiers ".part" (ceux qui contiennent les données à proprement dit), vous doublez l'espace disque occupé par chaque fichier en phase de téléchargement. La section inférieure vous permet de décider d'effectuer un backup en quittant le programme, ou après un certain nombre d'heures, et aussi d'écraser ou non les backups existants.



video etc.), avec eMule Plus, vous pouvez aussi spécifier les termes qui ne doivent pas apparaître dans le nom. La taille minimale et maximale du fichier recherché, le nombre de sources minimales et même son extension spécifique. Si en revanche vous n'avez pas la possibilité d'accéder à l'interface Web, vous

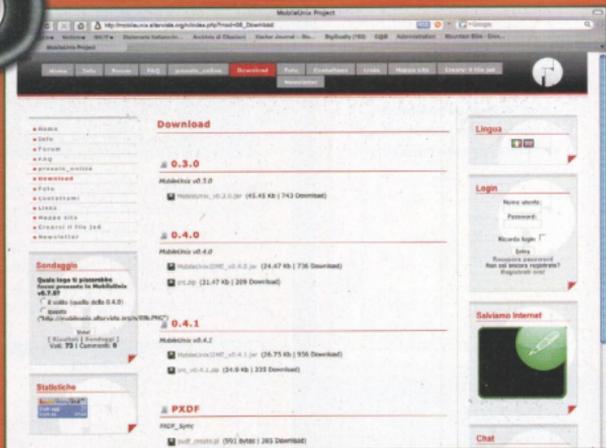
# MOBILEUNIX :



## Unix sur son portable

*Un système d'exploitation virtuel Unix-like, conçu pour une utilisation sur portables. Petit, maniable et en constante évolution !*

**U**n projet 100 % Italien dont le but est d'installer sur smartphone et portables de dernière génération, une version écrite en j2me du célèbre système d'exploitation. Avec MobileUnix (<http://mobileunix.altervista.org>), n'importe quel portable supportant la technologie Java peut en effet se transformer en console sur laquelle exécuter des commandes, même lorsque vous n'avez pas de PC. Comme le dit son auteur, Thomas Bertani, MobileUnix s'adresse avant tout aux petits débrouillards qui ne peuvent pas se passer de la ligne de commande, et aux professionnels qui doivent toujours emmener leurs fichiers partout sur leurs déplacements. Vous pouvez l'utiliser comme outil didactique pour vous rapprocher du shell



ou ne serait-ce que pour écrire des notes. A l'heure où nous écrivons, vous pouvez télécharger gratuitement la toute dernière version (la 4.0.) sur le site web, à la section download (<http://mobileunix.altervista.org/>

[n/index.php?mod=06\\_Download](http://mobileunix.altervista.org/n/index.php?mod=06_Download)), Vous y trouverez aussi la source et certains scripts en Python et en Perl pour créer, extraire et synchroniser le dump (nous en parlerons plus loin) en fichiers réels,



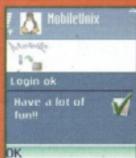
Une fois le téléchargement effectué, vous vous retrouverez avec un fichier appelé "MobileUnixJ2ME\_v0.4.0.jar" de 25 Ko seulement que vous devrez copier sur votre portable (ou sur un émulateur).

## :: Comment l'utiliser

Après avoir transféré le fichier portant l'extension .jar, il ne reste plus qu'à l'exécuter. Les données de login sont

User: 'root'  
Password: 'default'

Vous êtes maintenant dans le shell de



MobileUnix (/home/root) qui vous accueille par un message de bienvenue "Have a lot of fun", suivi de l'invite de root :

Sh:~ #

Avec 'man cmd', vous obtiendrez la liste des commandes implémentées et utilisables, standard et non standard qui, dans la version 4.0 sont : echo, pwd, cd, mkdir, rmdir, rm, ls, cat, man, logna-

me, uname, date, time, more, set, unset, alias, unalias, passwd, history, at, unat, muw, clear, de, mv, cp, di, tile, license. Pour plus d'informations, il vous suffit de taper 'man <nomcommande>'. L'une des commandes les plus intéressantes est 'muw', qui lance MobileUnixWriter, un éditeur pour créer, modifier et enregistrer des textes. Pour sortir de MobileUnix, on utilise en revanche 'halt' ou 'reboot' pour recommencer tout de suite.

## Le dump

Pour enregistrer les données et les informations de la session, il existe deux commandes spécifiques :

'-de', pour exporter le dump

Celui-ci doit être soit copié avec la fonction copier/coller et collé manuellement (uniquement possible sur Motorola et Nokia) soit envoyé par le biais d'un type quelconque de message : sms, mms ou e-mail (possible sur tous les téléphones).

'-di' est la fonction inverse et sert en revanche à importer le dump. Les dump sont conçus pour être gérés via PC, avec lequel il est possible synchroniser la session de MobileUnix. Et ce, grâce aux scripts téléchargeables à partir du site web. Pour créer ou extraire les dump, vous devez les exécuter en ligne de commande avec un interprète Perl (deux fichiers portant l'extension .pl) ou en Python (un unique fichier qui assure les deux fonctions).

## :: La version est servie !

La nouvelle version 4.0 de MobileUnix marque un nouveau pas en avant. Tout d'abord, l'exécutible est encore plus léger, en passant de 45 à 25 Ko, et son exécution est plus rapide. On note ensuite une plus grande stabilité et des améliorations dignes d'être soulignées comme un terminal plus Unix-like. Par rapport à la version 3, toujours disponible en cas de problèmes de compatibilité avec son smartphone, notons aussi un changement de licence pour le moins radical : la Creative Commons MobileUnix a en effet laissé place à la nouvelle GPL3. Améliorée ne signifie pas pour autant achevée ou exempte de problèmes : MobileUnix est en constante évolution et présente quelques bugs ici et là. Ainsi, la version 4.0 s'arrête parfois et n'accepte plus d'input : ça nous est

## L'INTERVIEW

Pour en savoir plus sur la genèse de MobileUnix, nous avons posé quelques questions à Thomas Bertani.

► La toute première version de MobileUnix

**HNM** : Comment le projet a-t-il vu le jour ?

**TB** : L'idée m'est venue en 2006, à Noël.

J'étais loin de chez moi et mon pingouin préféré me manquait. Vers la mi-janvier, j'avais terminé la première version (0.1.0).

**HNM** : Avec quels outils l'avez-vous développé ?

**TB** : Au début, j'ai développé avec mobilebasic. Les dernières versions ont été compilées avec midletpascal et je l'ai donc programmé un peu en pascal et un peu en j2me pur.

**HNM** : Sur quel portable l'utilisez-vous ?

**TB** : Sur un simple Sony Ericsson t630, mais pour faire des tests, j'utilise souvent un SE v800 (à ma mère) et un motorola v3xx (merci Matteo !)

**HNM** : Quelle a été la réaction du public après cette première version ?

**TB** : J'ai reçu de nombreux e-mails de remerciements de personnes vivant en France, en Russie et même au Pérou ! Je dois beaucoup à tous ceux qui m'ont soutenu ; sans eux, je n'aurais jamais eu ces précieux conseils !



## UN PROJET EUROPÉEN

Le site web d'un MobileUnix était forcément lié à un autre projet italien.

Le moteur utilisé par Thomas n'est autre que Flatnuke (<http://flatnuke.netsons.org/>), un CMS qui n'utilise pas de base de données mais stocke ces dernières dans de simples fichiers. S'inspirant de PHPNuke quant aux fonctionnalités et au layout, mais disposant aujourd'hui d'une personnalité qui lui est propre, Flatnuke est le fruit du travail et de l'inventivité de Simone Vellei, auxquels se sont ensuite adjoints Marco Segato et Aldo Boccacci. Le CMS bénéficie d'une base d'utilisateurs qui l'ont utilisé dans des situations très précises. Seule condition : qu'il s'agisse d'un serveur PHP.

arrivé avec la commande 'ls' mais certains cas dans le forum ont évoqué un problème avec la commande 'passwd'. Parfois, le problème peut être lié au modèle de portable (ici un SE v2101). La meilleure chose à faire, c'est de le signaler au développeur qui analysera le problème et prendra les mesures qui s'imposent en sortant ensuite une nouvelle version.

Nicola D'Agostino



# SÉOUL, 6H DU MAT LES PIRATES SE REVEILLEN

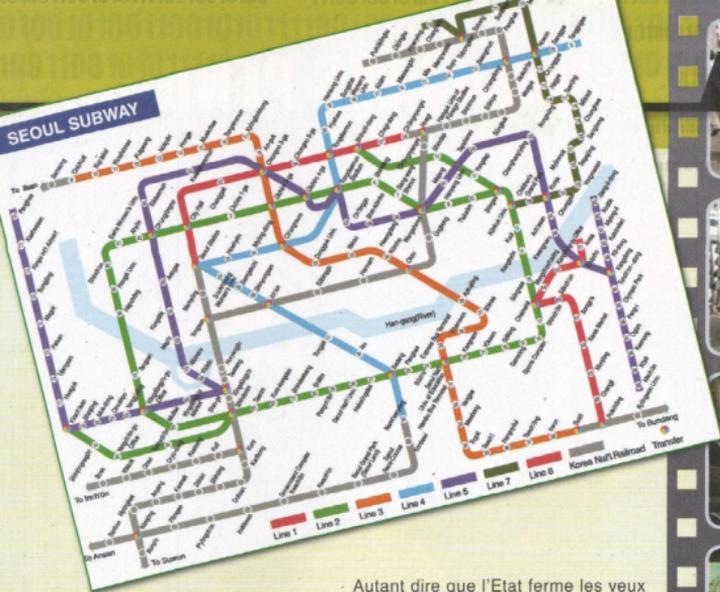
*Les majors du disque et du cinéma s'attaquent aux pirates informatiques. Ils le crient haut et fort au points d'imposer aux législateurs de voter des lois à la limite du liberticide.*

Par Damien Banaud

**I**l fait chaud, très chaud même. L'humidité et la moiteur de l'air en ce début de journée sont assez étonnantes. Il est 6 heures du mat', Eric Romang et moi sommes à Séoul, dans un quartier où l'informatique est reine. Ne nous demandez pas l'adresse, les noms de rues en Corée, ça n'existe pas. A quelques pas du quartier de l'Us Army, prenez des dizaines d'immeubles, saupoudrez le tout de plus de 6.000 boutiques et vous voilà dans l'un des plus gros capharnaüm électronique qu'il nous a été donné de voir. Nous sommes au Yong-San Electronics Market et l'ambiance électrique n'est pas un vain mot. Dans les rues, partout, des tentes. Des stands en plein air feraient pâlir le moindre enquêteur de la RIAA, MPAA, BSA, ... Des milliers, voir des dizaines de milliers de contrefaçons de films, logiciels, albums de musique sont écoulés, chaque jour, dans ce marché à ciel ouvert. Des films très récents, voir pas sortie en salle, à des prix qui laissent pantois.

Le business semble être fleurant car les «commerçants» proposent quatre DVD pour un peu plus de 8 euros (10.000 wons). A partir d'un catalogue, et des boîtes vides, les vendeurs prennent votre commande, ils téléphonent ensuite à un





«fournisseur» qui, quelques minutes plus tard, ramènent les DVD gravés. Le vendeur n'a plus qu'à installer les jaquettes dans les boîtes et le tour est joué ! Les films ? Des copies trouvées sur Internet, sur le P2P, mais aussi, via des accès warez qui approvisionnent ces pirates en contenus frais. Nous avons d'ailleurs pu découvrir que certaines productions pirates étaient estampillées « Made in China » ou encore du nom de groupes warez très connus dans la scène underground internationale,

## :: Que fait la police ?

«Ils descendent très rarement ici, explique un vendeur, deux à trois fois par ans. Quand ils viennent, ils cassent tous, on a une grosse amende et puis tout rentre dans l'ordre le lendemain». Autant dire que la peur du «gendarme» n'est pas vraiment à l'ordre du jour. « Ils viennent aussi brûler les jaquettes, confiait un autre vendeur. Nous n'avons jamais de DVD avec nous, donc ils repartent et nous laissent tranquille ».

Autant dire que l'Etat ferme les yeux sur ce « marketing » juteux. Il n'est pas bien compliqué de prouver que tout ceci est de la contrefaçon pure et dure. Nous nous sommes amusés à calculer le chiffre d'affaires d'un stand, sur une journée. Avec une vingtaine de clients par heure, un stand peu touché plus de 3,000 euros... et il y a des centaines de stands !

Les vendeurs ont-ils peur de la RIAA, MPAA, BSA ? Si c'est le cas, les commerçants cachent bien leur jeu. D'autant plus qu'à quelques pas du Yong-san Electronics Market, et de ses tentes, se trouve le quartier militaire des troupes américaines basées à Séoul. « De très bons clients » rigolent encore les vendeurs que nous avons interrogé.

Bref, vous l'aurez compris, pendant que les majors tapent sur des pays comme la France, le Canada, l'Asie (dont la Chine) continue de fournir le monde en millions de copies. Eric connaît très bien la Corée-du-Sud, il y a deux ans, les copies Chinoises n'étaient pas aussi nombreuses, aussi visibles. «C'est devenu fous complètement fou» confirme-t-il. Et à première vue ce n'est pas prêt de s'arrêter. ■

## ENQUETE



# EN ROUTE POUR SÉOUL

# LES HACKERS AIMENT LES PENGUINS

Découpez et collez les pièces en suivant les numéros

