

DÉJÀ 7 PATCHS POUR VISTA !!!

0% DE PUBLICITÉ
JUSTE DES ARTICLES
2€

www.hackernowmag.it
HACKER
news
Magazine

Avec John the
RIPPER,
les **MOTS DE PASSE**
n'ont qu'à bien se tenir !

DEFENDEZ VOTRE LIBERTÉ INFORMATIQUE

Le programme
antipiratage de
Windows

Windows Genuine Advantage

**TRANSFORMÉ EN
PASSOIRE PAR
WGA FUCKER !**

Vengeance de
HACKER

Les 3 règles pour
**COINCER CEUX
QUI VOUS
ATTAQUENT**



**INTERVIEW
EXCLUSIVE**

VISTA
déjà dans le
PÉTRIN !

Interview de celle qui a
INFECTÉ le tout nouveau
SYSTÈME D'EXPLOITATION

Année 2 - n°17
Bimestriel
Avril / Mai 2007

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"

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
Brugués, 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 Arsenà

Mise en page : Selestudio Srl

Coordination : Alessandra Calò

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'engage que la
responsabilité de leurs auteurs.
Sauf accord particulier et publiés ou non, ils
ne sont pas renvoyés.

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

Editorial

HACKER
Magazine

Le beurre et l'argent du beurre

Ah ! La sagesse des anciens... Eux, au moins, savaient que l'on ne peut pas avoir une chose et son contraire.

Pourtant, Lionel ne l'a toujours pas compris. Il me prend sur le chat et me dit : Comment est-ce que je dois faire pour partager ma connexion ADSL avec un ami qui habite à côté de chez moi ? Si j'ai une connexion ADSL sans fil et que lui, a une carte sans fil, il pourra se connecter ? Je lui réponds que ça marchera à coup sûr. Mais n'oublie pas que c'est illégal, techniquement parlant. Ah Oui ? Bon, ok me répond Lionel. De toute façon, personne ne s'en rendra compte. C'est toujours les mêmes lois stupides. Et au final, c'est moi qui paie, alors c'est moi que ça regarde, non ? s'énerve-t-il.

Je suis d'accord avec toi, lui dis-je. La loi est stupide, mais ton voisin fait peut-être partie de la Répression des fraudes, j'en sais rien moi. C'était juste pour te donner une réponse précise.

Silence. Dans un chat, les silences sont toujours pesants, même lorsqu'ils ne durent en réalité que quelques instants. Un silence qui paraît une éternité. Et qui laisse présager autre chose. J'attends.

Je peux te poser une question ?

Bien sûr que tu peux ! On est là pour discuter. Si je peux te répondre, je le ferai.

Nouvelle pause, puis il écrit : comment faire pour savoir quand il est connecté ?

Je ne comprends pas. Je lui réponds : eh bien, tu peux logger le router, ou tu peux aussi sniffer ton réseau... Mais s'il se connecte quand toi du dors ? Nouvelle pause. Non, ce n'est pas pour lui... mais comment est-ce que tu fais pour savoir si quelqu'un d'autre ne s'est pas connecté ?

Cette fois, c'est moi qui fais une pause. Tu n'as qu'à restreindre l'accès en fonction des adresses MAC et faire en sorte que ton réseau n'accepte que tes ordinateurs, plus celui de ton voisin.

Ah ! me répond-t-il. Mais il n'existe pas quelque chose de plus précis ?

Je commence à perdre patience. Si tu as peur de ce que peut faire ton voisin avec ton réseau, alors pourquoi est-ce que tu veux l'autoriser à s'y connecter ? Sur le ton de quelqu'un qui avouerait un triple homicide, il conclut : tu sais, on ne sait jamais...

Il est sympa Lionel, mais trop de gens raisonnent comme lui. On prétend à une liberté absolue, quitte à contourner les lois lorsqu'elles sont stupides, et même quand elles ne le sont pas. Et puis ensuite, on veut avoir le contrôle total. Même sur notre voisin. Et si lui aussi voulait contourner quelque chose que nous estimons stupide ? Non, pas lui ! Les seuls qui peuvent faire les malins, c'est nous !

Alors, quel rapport entre tout ça et les hackers ? me demanderont certains. Le rapport est évident.

Les hackers luttent pour défendre leurs droits, vaillamment s'il le faut. Justement parce qu'ils sont conscients de leurs devoirs. Ils luttent pour l'égalité des connaissances, contre les privilèges et les privilégiés. Ce ne sont pas eux, les fauteurs de troubles. Ce sont eux par contre, qui les démasquent.

Cette année est placée sous le signe du hacking. Nous sommes en mission pour la liberté de tous. Et pas dans notre propre intérêt. Ne l'oublions jamais !

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

HACK NEWS

Événements et nouvelles d'un monde devenu fou !

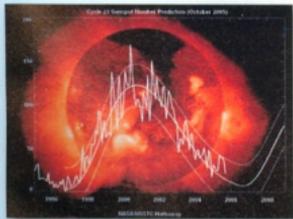
Communications HS (cette fois la censure n'y est pour rien !), systèmes de reconnaissance d'empreintes digitales et autres logiciels détecteurs de mensonges qui eux, ont tout de la censure.

:: Panique en Chine

Une tempête de particules subatomiques a déferlé à des millions de kilomètres de nous, après une éruption solaire. Le flux des particules est arrivé sur Terre le 14 décembre, en faisant sauter les communications téléphoniques, les signaux de navigation GPS et plus généralement ceux à ondes courtes, sur l'ensemble du territoire chinois.

Même la station spatiale ISS en a ressenti les effets et le software et les données qui permettent de bien positionner le système ont dû être réinstallés depuis la Terre, car les puces mémoire sont particulièrement sensibles aux particules subatomiques, qui les traversent en détruisant les données.

Les astronautes ont été en revanche avertis à temps et ont pu se réfugier dans un local spécifique à l'épreuve des radiations, en attendant que le vent passe. Et si ce flux avait également effacé notre compte en banque ?



▲ Explosions solaires, la terreur des puces électroniques.

:: Système portable de reconnaissance digitale

Les patrouilles de la police de Columbus, dans l'Etat de l'Ohio, ont été équipées d'un système de reconnaissance d'empreintes digitales capable de les transmettre par WiFi à une base de données centrale, pour une reconnaissance instantanée. Seul hic : si nous ne sommes pas fichés,



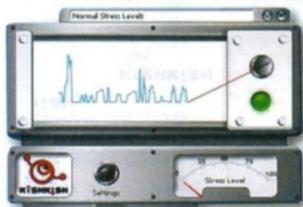
la police en profiterait-elle pour nous intégrer dans sa base de données ? Si nous sommes arrêtés et que l'on contrôle également nos empreintes, allons-nous peupler à notre insu

« Génial, un contrôle approfondi en temps réel. Mais s'ils ne trouvent rien, serons-nous toutefois fichés à notre insu ? »

une base de données qui auparavant ignorait jusqu'à notre existence ? Hum ! Voici une question qui mérite qu'on s'y penche...

:: Skype vous juge !

KishKish Lie Detector est un add-on que vous pourrez installer très prochainement sur Skype. Objectif ? Déterminer à partir de l'empreinte vocale si l'on vous ment. Oups ! Un programme qui a priori peut être amusant, mais qu'en est-il si à cet instant nous sommes stressés ? Et s'il se trompait, tout simplement parce que notre timbre de voix n'est pas intégré aux paramètres



▲ Tout le monde vante ses mérites. Nous, on s'en méfie comme de la peste !

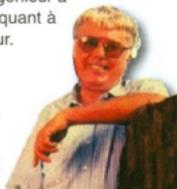
du fabricant ? Le fait qu'une personne nous refuse sa confiance uniquement parce que nous lui avons parlé sur Skype et non sur un téléphone normal, est plutôt révoltant !

Mais au final, peut-être que non : car si quelqu'un se fie à ce système uniquement pour savoir si vous êtes un ami, alors mieux vaut le laisser tomber ! Légende : Tout le monde vante ses mérites. Nous, on s'en méfie comme de la peste !

:: Souvenir, souvenir...

On s'en souviendra comme de l'homme du disque dur : Alan Shugart, fondateur de la société Seagate Technology, est décédé le 12 décembre en nous laissant le souvenir de son premier disque de 5 Mo. Dès le début de sa carrière, commencée chez IBM, il s'est intéressé aux mémoires de masse, en inventant, avec son équipe, la disquette. Le monde a perdu un grand ingénieur à qui l'on doit beaucoup quant à l'évolution de l'ordinateur. Merci, Alan !

► Dommage qu'il ne reste de lui qu'un souvenir dans les musées. Et quelques petites photos détraquées...





2 VERS POUR MOBILES

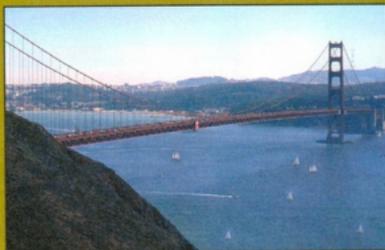
La présence de deux bugs sur des appareils mobiles équipés de Windows Mobile, pourrait bien en faire des victimes faciles d'une attaque par déni de service. Mais nous ne sommes pas les seuls à le dire, Trend Micro l'affirme également. Ces vers concernent les versions 5.0 et 2003 du système d'exploitation et frappent Internet Explorer et Pictures and Video. Le premier, de type stack overflow est activé par l'ouverture d'une page Web peu scrupuleuse et ferme le navigateur, outre le fait de déstabiliser le système. Le second part avec un jpeg et gèle le système pendant 10 à 15 minutes. Rassurant, non ?

PAYEZ

VOS PRUNES!

Si se prendre une prune est toujours une expérience désagréable, on est souvent tenté de ne pas la payer. A San Francisco, échapper aux contraventions pourrait devenir beaucoup plus difficile. La ville est en effet en train d'expérimenter un nouveau système pour coincer toutes les personnes n'ayant pas payé leurs amendes pour stationnement interdit. En janvier et février, deux voitures équipées de caméras patrouilleront dans les rues de la ville californienne ; ces caméras vidéo

sont capables de relever les numéros d'immatriculation des voitures (jusqu'à 250/heure) et de les comparer à la base de données de toutes les personnes n'ayant pas réglé leurs amendes. Une fois le fraudeur découvert, les policiers bloquent sa voiture jusqu'au paiement des arriérés. Les contraventions rapportent environ



Interdiction de stationner sur Golden Gate !

85 millions de dollars par an à la ville de San Francisco et il est donc primordial d'inciter les gens à les payer. Après cette phase expérimentale, le système sera définitivement adopté et diffusé, du moins s'il donne les résultats escomptés.

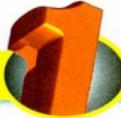
ÇA NE RIGOLE PAS !

Les autorités de la Corée du Sud, très paranos ces derniers temps, ont annoncé qu'elles avaient arrêté deux spammeurs accusés d'avoir contaminé au moins 12 000 utilisateurs dans la péninsule asiatique. Les deux jeunes gens, l'un âgé de 20 ans et l'autre de 26 ans, dont les noms n'ont pas été communiqués, se seraient adonnés à des techniques courantes de phishing avec lesquelles ils auraient recueilli les données confidentielles d'utilisateurs, ensuite revendues à des entreprises étrangères moyennant une rétribution d'environ 95 000 euros.

LINUX PUNI ?

Imaginons par pur hasard que vous souhaitiez suivre en streaming les séances du Parlement européen et que vous utilisiez une version quelconque de Linux. Eh bien ! vous ne pourriez pas exaucer votre vœu. Le service de streaming n'est en effet disponible que pour les utilisateurs de Windows et de Macintosh. L'explication fournie par l'Union européenne est très étrange : "Il est impossible de soutenir Linux en toute légalité", une phrase en effet plutôt bizarre. Si





HOT NEWS

DES CHAUSSURES CATALOGUEES

Le Royaume-Uni traverse une véritable vague de répression. Et les nouvelles sont de plus en plus inquiétantes: d'après certaines, non seulement, des caméras vidéo à rayons X seront installées un peu partout dans les rues de la capitale britannique ainsi que des capteurs capables de "flairer" la présence d'explosifs, mais une gigantesque base de données d'empreintes de chaussures scannées verra également le jour. Cette trouvaille devrait aider les forces de l'ordre anglaises à tracer des criminels et suspects sur la base d'éventuels indices retrouvés sur les lieux du crime. L'empreinte du pied, la façon dont celle-ci est modifiée par le type de chaussure, le poids corporel et le type de démarche semblent en effet constituer tous les paramètres permettant d'identifier distinctement une personne d'une autre.

VOUS VIVEZ A ROME ?

Si la réponse est oui (la banlieue est également comprise) et que vous avez entre 18 et 24 ans, n'hésitez pas à participer à un intéressant concours, appelé "Aujourd'hui, c'est moi qui programme", lancé par la Province de Rome. En résumé, il s'agit d'écrire un programme destiné aux écoles ou à l'administration publique. Les trois vainqueurs recevront respectivement des prix de 4 500, 2 500 et 1 000 euros. L'aspect le plus intéressant de ce concours : la création d'un software libre, c'est-à-dire respectant la licence GPL. Les projets primés seront donc librement téléchargeables et utilisables. Si vous avez toutes les conditions requises, alors, allez-y, retenez vos manches ! Dernier délai pour présenter son software : le 31 mars 2007. Vous trouverez l'avis complet du concours sur le site de la Province de Rome, à la page <http://snipurl.com/16dgg>.

LINUX BOSSE GRATUITEMENT !

La diffusion du pingouin sur les ordinateurs du monde entier semble être au creux de la vague mais les développeurs ne baissent pas les bras pour autant et revien-

nent sur le devant de la scène avec une proposition intéressante : développer gratuitement les drivers pour le compte de chaque fabricant. En échange, ils ne deman-

dent que des spécifications de fonctionnement du dispositif sur lequel le pingouin devra aller ou un technicien qui puisse fournir des explications. Intéressant, non ?

PRETS POUR LE WIMAX !

L'heure est enfin venue pour l'Italie ! Les Ministères de la Défense et des Communications ont récemment conclu un accord qui permettra d'utiliser à des fins civiles certaines fréquences jusqu'alors réservées aux communications militaires. Cet accord devrait être le point de départ pour lancer cette technologie même en Italie. L'un de ses principaux avantages : pouvoir amener le Haut Débit dans des zones ne bénéficiant toujours pas des traditionnelles liaisons par câble. Les premières licences devraient être données à partir de juin, après les principaux Pays européens, comme la Grande Bretagne, l'Allemagne et la France, où le WiMax est déjà opérationnel depuis longtemps...



FIN DE LA PRESSE PAPIER ?

Selon l'éminent Institut de recherche Carnegie-Knight Task Force, les heures de la presse papier seraient comptées. Les utilisateurs qui se fient à des sources journalistiques et d'information on-line sont de plus en plus nombreux. Facilité de repérage, qualité, rapidité pour diffuser l'information et la possibilité d'effectuer des recherches thématiques rapides et détaillées, sont les éléments pour lesquels les lecteurs semblent avoir une prédilection. Mais pas seulement ! Sur un échantillon de jeunes, tous étudiants des écoles supérieures américaines, 75 % ont déclaré qu'ils ne pouvaient même pas supporter l'idée de consulter un journal traditionnel pour rechercher des informations. Alors, devons-nous réaliser un Hacker New Mag. version télématique ? Ça pourrait être une idée... Mais, pour d'instant, notre mag se porte bien !

vous souhaitez que l'UE change de comportement, vous pouvez signer une pétition online que vous trouverez à la page <http://snipurl.com/16cpcy>. Et donnez-nous ensuite des nouvelles des passionnants débats de Strasbourg.





TELEOBJECTIF POUR PORTABLES

Une idée qui devrait plutôt bien fonctionner avec les téléphones portables dernière génération, avec quelques mégapixels en plus. Il s'installe en un tour de main, ne prend pas de place, coûte peu et vous permettra de rapprocher les personnes les plus éloignées. Dans les concerts ? Génial ! Pour éviter de prendre les sempiternels panoramas archi vus et revus et partir à la chasse de petits détails ? C'est possible ! Ne vous attendez pas à une qualité de lentille mirabolante, mais pour s'amuser, ça suffit amplement !

Lien utile : <http://mobile.brandoo.com/hk/MobilePhoneTelescope-Nokia.php>

LA WI-FI

CEST SANS DANGER !

De temps à autre, quelqu'un surgit de l'horizon et s'inquiète de la santé de toutes les personnes utilisant des réseaux wi-fi, en les terrorisant avec des données alarmistes : le fait d'être prêt d'un routeur sans fil reviendrait à vivre dans un réacteur nucléaire. Un article publié dans le Times, que vous pouvez également lire on-line sur <http://snipurl.com/1549g>, tente de faire le point sur la situation. D'un côté, les écoles autrichiennes et canadiennes ont décidé de bannir totalement la wi-fi de leurs bâtiments. De l'autre, le Dr Michael Clark, de la Health Protection Agency (Agence pour la protection de la santé), soutient en revanche que les radiations provenant de la wi-fi sont beaucoup plus faibles que celles émises par les téléphones portables. Selon lui, une année passée dans une classe d'école à côté d'une base wi-fi équivaldrait à 20 minutes de communication

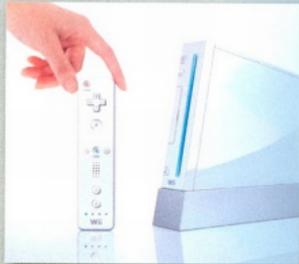


▲ Ce logo remplacera-t-il le panneau danger ?

sur un téléphone portable. Pourtant, on voit tous les jours des gens qui parlent pendant des heures sur leur portable sans s'inquiéter et on doit subir parallèlement les tirades de ceux qui "s'inquiètent" de notre santé et souhaitent nous éloigner des ordinateurs et autres réseaux. Bref, un peu de bon sens serait le bienvenu, une denrée rare de nos jours...

Wii, DES CORDONS TROP FRAGILES !

Les cordons de la Nintendo Wii cèdent sous l'action des gestes dynamiques des joueurs. La société devra en remplacer au moins trois millions. Après les crashes des télécommandes sur des écrans Lcd, Nintendo a été contrainte d'agir vite, avant qu'il ne soit trop tard. Une excellente preuve du sérieux commercial, mais un flop sensationnel quant à la conception d'un matériel si banal. Comme quoi, même les meilleurs se trompent !



▲ La console Wii nous présente ses premiers, et nous l'espérons, ses derniers problèmes.

OFFRE D'EMPLOI BIDON

Le phishing continue à faire des victimes. Dans le cas présent, il s'agit d'un e-mail qui propose des offres d'emploi avec un salaire d'environ 2 500 euros/mois à un nombre très limité de candidats potentiels, seulement 32 voire moins (nous avons vu différentes versions de cette offre). L'arnaque consiste bien sûr à vous faire remplir un formulaire on-line (par exemple à l'adresse-bidon qui

HOT NEWS

VOUS PARTAGEZ ? ALORS VOUS ÊTES COUPABLE ! FSF CONTRE VISTA

Ainsi en a décidé un juge américain, en donnant raison à la Riaa, l'association des disques américains. Dans la pratique, la décision de ce juge est une première, dans la mesure où il a établi qu'il n'y avait pas de différence, d'un point de vue juridique, entre partager de la musique et la télécharger. C'est justement sur cette différence que s'était basée la défense de Dave Perez, qui avait partagé certains fichiers sur le réseau de Kazaa : d'après ses avocats, on ne peut pas parler de délit tant qu'on n'a pas prouvé que le matériel a été téléchargé au moins une fois. Le juge a toutefois donné raison à Riaa. Une décision qui, dès à présent, va mener la vie dure à ceux qui souhaitent partager musiques et films. Espérons que la nouvelle ne parviendra pas aux oreilles de nos législateurs...

FSF, Free Software Foundation, a lancé une campagne destinée à dévoiler aux utilisateurs d'ordinateurs les dangers liés à Windows Vista et à les convaincre de passer à l'utilisation de systèmes d'exploitation et software open source. Selon FSF, Vista marque un pas en arrière par rapport au contrôle que l'utilisateur peut exercer sur sa machine. C'est pourquoi, il est important de s'en rendre compte et de chercher des alternatives qui puissent nous libérer de Microsoft. Vous pouvez suivre cette campagne sur le blog : <http://badvista.fsf.org/>, toujours mis à jour et plein de ressources intéressantes. Alors, soutenons-la !



LA FORCE DE L'ESPRIT

Un groupe de scientifiques de l'Université de Washington a réussi à faire en sorte qu'un robot obéisse à certains ordres donnés par les biais d'impulsions cérébrales. La personne chargée de

guider le robot portait un casque avec des électrodes capables de capter les ondes cérébrales. Pour l'instant, le robot n'a été capable que de se déplacer en avant, ramasser un ou deux objets et les bouger, mais

les scientifiques sont confiants quant aux évolutions à venir. Vous trouverez un compte-rendu détaillé de cette dernière invention, en anglais, à l'adresse suivante : <http://snipurl.com/1543m>.

TIMES

Faute de mieux, la célèbre revue américaine, qui, tous les ans désigne la "Person of the Year", révolutionne cette année son concept : ce qui l'intéresse, ce n'est plus la personne seule, célèbre de par son impact positif ou négatif sur le monde, mais YOU, c'est-à-dire "toi" ou "vous", donc tous ceux qui connaissent et utilisent les nouvelles technologies (mais si on les appelle ainsi depuis des années, sent-elle au final si nouvelles?). L'hebdomadaire ne pouvait ignorer les nouveaux succès de cette année, du boom de YouTube à MySpace, pour ne pas dire Wikipedia, tous unis par le fait qu'ils ne pourraient exister sans Internet. Les véritables protagonistes de 2006 sont donc toutes les personnes qui, tout doucement changent le monde en devenant personnellement des protagonistes de l'information et du partage d'informations, de photos, faits et événements. Bien sûr, nous en faisons également partie, nous les hackers, même si bon nombre de personnes pensent le contraire. Pour lire les motifs officiels de cette nomination, connectez-vous sur <http://snipurl.com/1531s>.

MARRÉ DES JEUX VIDÉO VIOLENTS

En novembre dernier, Sebastian Bosse un jeune Allemand de 18 ans, est entré dans une école, a blessé 37 personnes puis s'est donné la mort. La faute à qui ? A Counter-Strike, selon certains politiciens allemands. Le jeune homme était semble-t-il si passionné, qu'il en a perdu le sens des réalités et ne s'est pas rendu compte de ce qu'il faisait. Certains députés de Bavière et de Basse-Saxe ont présenté une proposition de loi selon laquelle les fabricants tout comme les utilisateurs de jeux vidéo violents à l'égard d'êtres humains, pourraient être considérés comme responsables d'éventuels crimes inspirés par les jeux. Les peines devraient aller de simples amendes à un an de prison. Les fabricants, quant à eux, organisent leur défense contre cette énième chasse aux sorcières ! Mais ne vaudrait-il pas mieux soutenir les familles et aider les jeunes ?

vous refiler – attention !! – un malware quelconque : www.xread.biz/offer-t/index.html) avec toutes vos données, ou encore à répondre à l'e-mail avec les mêmes données personnelles. Si vous n'êtes pas intéressé, vous êtes alors invité à répondre quand même pour éviter d'autres envois...

Au mieux, on vous confirme la validité de votre adresse e-mail pour vous envoyer des spams à n'en plus finir. Tout le reste, n'est que pure malhonnêteté !

La MAGICIENNE du rootkit

Pour Joanna Rutkowska, les anti-virus sont inutiles et les machines virtuelles un danger. Voici ses explications !



Ceux qui ne connaissent pas Joanna Rutkowska ont de quoi s'inquiéter ! Car il s'agit en effet d'une experte dans l'art de passer inaperçu, surtout lorsqu'il s'agit de rootkit et de malware (codes malveillants). Ces derniers mois, Joanna a défrayé la chronique lors de la Conférence Black Hat, où elle a montré comment infecter Windows Vista avec un rootkit et présenté Blue Pill, un nouveau genre de rootkit exploitant une technologie de virtualisation pour créer un malware 100 % indétectable. Joanna est un personnage des plus intéressants et mérite qu'on l'écoute.

Hacker Magazine : Qui êtes-vous ?

Joanna Rutkowska : Je suis une chercheuse spécialisée dans les technologies furtives et la détection d'attaques. Je m'occupe de rootkit au niveau du noyau (kernel), de codes malveillants furtifs et de communications cachées de réseau. Je vis à Varsovie en Pologne et travaille pour COSEINC, une société spécialisée dans la sécurité informatique dont le siège est à Singapour.



HM : A quel âge avez-vous eu votre premier ordinateur ? Vous pouvez nous le décrire ?

JR : J'avais 11 ans. C'était un PC AT-286, avec 2 Mo de RAM et un disque dur de 40 Mo (oui, mégaoctets !). Pour l'époque, c'était une bête de course, mais la carte graphique n'était pas bonne et comme on ne parvenait pas à jouer, j'ai donc commencé à apprendre le langage BASIC et la programmation. Par la suite, j'ai travaillé sur la façon d'agir et se défendre après une attaque réussie : backdoor dans le noyau, rootkit, canaux de transmission cachés et ainsi de suite.

HM : Quel est votre système d'exploitation ? Et utilisez-vous un logiciel de sécurité ?

JR : La mia macchina principale usa Windows XP x64. Non uso Mon ordinateur principal utilise Windows XP 64 bits. Je n'utilise aucun anti-virus, car je n'aime par leur approche. Ils bloquent uniquement le malware qu'ils connaissent. Je ne crois pas non plus aux systèmes de détection d'intrusions. De temps à autre, je contrôle mon trafic avec Wireshark pour voir si tout est en ordre et puis, je fais très attention !

HM : Quant avez-vous fait la connaissance des rootkit ?

JR : Au lieu de penser à la façon de prendre le contrôle du système, j'ai pensé à ce qu'il fallait faire après. J'ai découvert l'existence de certains rootkit pour Linux comme Knark ou Adore et j'ai commencé à m'interroger sur la façon dont j'aurais pu m'apercevoir de leur installation.

HM : Créer un rootkit offensif n'aide-t-il pas les personnes malintentionnées ?

JR : Non, ça incite les personnes honnêtes à développer des défenses toujours plus efficaces.

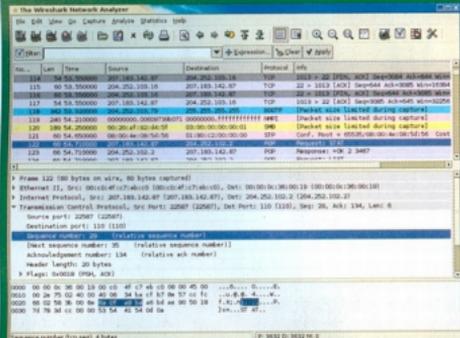
HM : D'après vous, les détails d'une attaque doivent-ils être rendus publics ?

DEFINITIONS

Un rootkit est un programme capable de s'allouer les privilèges d'administrateur, autrement dit de contrôler totalement un système. Virtualisation signifie créer une mémoire virtuelle sur laquelle on fait tourner un véritable ordinateur en miniature imperméable au reste de la mémoire et au système d'exploitation qui commande le reste de l'ordinateur. Si une machine virtuelle se trouve dans votre ordinateur, vous pouvez l'éteindre mais pas altérer son contenu depuis l'extérieur... à condition d'être au courant de son existence.

WIRESHARK!!!

Ethereal, l'analyseur de trafic par excellence, a changé de nom et s'appelle désormais Wireshark : <http://www.wireshark.org>. Ses capacités sont toutefois toujours les mêmes, excellentes !



▲ Légende : Wireshark fonctionne sur tous les ordinateurs et tous les systèmes d'exploitation les plus répandus, et il est open source. Alors heureux ?

JR : Oui, quand c'est utile pour développer une meilleure défense. Dans le cas de Blue Pill, connaître sa source ne serait d'aucune utilité, c'est pourquoi je n'ai pas révélé son code au grand jour. Dans d'autres cas, mieux vaut le faire, surtout si ça incite Microsoft à créer un patch !

HM : Considérez-vous les rootkit via une machine virtuelle comme une attaque dangereuse ? Et si oui, pourquoi ?

JR : La virtualisation est une technologie très puissante et toute nouvelle, il est important de comprendre à quel point elle peut être dangereuse. Blue Pill en est la preuve : un petit programme qui crée une machine virtuelle dans le hardware, puis transpose le système d'exploitation où Blue Pill a été lancé dans cette même machine virtuelle, tandis qu'il assure des pouvoirs de superviseur. Le tout dure environ un millième de seconde et le système d'exploitation ne se rend même pas compte qu'il a été intégré à une machine virtuelle. Des programmes comme Blue Pill pourraient être bloqués si le système d'exploitation disposait de son propre superviseur... Mais à l'heure actuelle, il n'en possède pas et plusieurs années pourraient s'écouler avant qu'on aboutisse à un tel progrès.

HM : Greg Hoglund, un expert en rootkit, a déclaré qu'un rootkit exploitant la technologie de virtualisation ne constituait pas une véritable menace. Etes-vous d'accord ?

JR : Il se réferait sans doute aux rootkit basés sur une virtualisation software, comme SubVirt. C'est tout à fait différent de ceux exploitant la virtualisation hardware, comme Blue Pill ou Vitriol de Dino dai Zovi (<http://www.matsano.com>). De nombreux "experts" diront que ce danger n'existe pas parce qu'ils ne le voient pas, dans la mesure où le rootkit parvient à se cacher parfaitement...

HM : Comment Microsoft a-t-il réagi face à votre attaque contre Vista ?

JR : J'ai fait part de trois solutions possibles, en déconseillant l'une d'elle car ce n'est qu'une solution temporaire. Dans la version la plus récente de Vista que j'ai eu entre les mains, c'est justement celle-ci que Microsoft a adoptée.

HM : Comment pensez-vous des scanner de rootkit qui existent actuellement ?

JR : Comme je l'ai dit, je ne les aime pas. Ils cherchent des programmes malveillants au lieu de se préoccuper de l'état général du système. Ils doivent par exemple chercher des processus cachés, quand on peut créer un malware furtif très puissant sans même faire partir un processus. La menace avec Blue Pill, c'est qu'il ne modifie pas même un bit du noyau. On peut ainsi contrôler tous les processus du monde alors que le rootkit est là, juste assis sur les contrôleurs !



HM : Le malware furtif doit-il nous inquiéter ? Pensez-vous que cette menace grandira ?

JR : Ce type de malware est inquiétant car il leurre la totalité du système d'exploitation, lequel devient totalement instable et peu fiable, par définition. En cas d'attaque sérieuse, il n'existe même pas de méthode valable pour savoir si le système a été compromis ou non.

Que la menace grandisse ou non, ce n'est pas ça l'important. Qu'importe si 100 ou 100 millions d'ordinateurs seront attaqués ou non. Ce qui est important c'est que ces attaques sont possibles et dangereuses. Nous devons faire quelque chose pour les arrêter avant que la technologie adaptée finisse entre de mauvaises mains. Et on doit agir vite !

David Nool
davenool@gmail.com

THE INVISIBLE WOMAN

Joanna Rutkowska tient à jour ses recherches sur un blog, Invisible Things, publié à l'adresse suivante : <http://theinvisiblethings.blogspot.com/>.

Frayer-vous un CHEMIN !

Vous avez égaré votre mot de passe ? Pas de panique ! Jtr est là pour vous le récupérer... et c'est l'un des meilleurs en la matière !



Salut à tous ! Je vous présente mon nouveau copain, il s'appelle John. Non, je vous en prie, pas d'arrière-pensées ! Ce n'est pas un homme, c'est un programme ! Son nom ? John the Ripper, et c'est l'un des meilleurs programmes de décryptage de mots de passe que je connaisse. Voici en deux mots un exemple de la façon dont vous pouvez l'utiliser. Deux mots qui pourraient bien s'éterniser à travers un long discours, mais 1) je ne veux pas être ennuyeuse, 2) cet article n'est là que pour vous ini-

tier car un vrai hacker approfondit toujours un sujet et n'attend pas que ça lui tombe du ciel, pas vrai ? Supposons que vous ayez oublié un mot de passe important dans votre ordinateur et que vous ayez à votre disposition le fichier hash des mots de passe. Supposons qu'il y ait dans ce fichier un hash du genre :

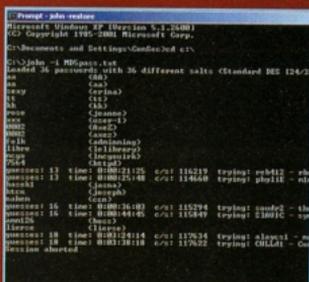
blah:S2XsgkWEIE9w

Voici toutefois certaines commandes de base :

```
John -si [passfile]
John -w : [wordlist][passfile]
John -i [passfile]
```

Si vous utilisez Windows et que John se trouve dans votre répertoire C : tapez

C:\john -i md5pass.txt



TROUVEZ LE FICHER

Windows NT, 2000 et XP, n'intègrent pas de fichier de mots de passe. Ces derniers sont toutefois enregistrés sous forme cryptée dans le Registre de Windows. Un programme comme PWDump de Jeremy Allison (<http://snipurl.com/13h0z>) pourra vous afficher les données en question. Le mot de passe reste toutefois crypté et John the Ripper prouve une nouvelle fois son utilité. Sur les systèmes Unix, les mots de passe, toujours cryptés, sont regroupés dans un fichier qui pourrait se nommer ainsi /etc/passwd.

▲ La syntaxe de John the Ripper peut être très simple, comme celle présentée ci-dessus.

Le travail de John consiste à transformer ce hash incompréhensible en un mot de passe compréhensible.

:: Des commandes pour tout type d'usage

John dispose de différents modes d'action. Pour les découvrir tous, n'attendez plus et plongez-vous dans sa documentation.

▲ En appuyant sur une touche pendant l'exécution, vous pourrez savoir à quel stade en est le programme. Ctrl + C interrompt l'exécution.

"md5pass.txt" est le fichier de mots de passe sur lequel nous souhaitons travailler, et qui pourrait bien sûr se nom-

WGA sur la sellette !

Peu pratique, envahissant et gênant : c'est le moins qu'on puisse dire de ce programme de vérification de licences de Microsoft. Mais quelqu'un a eu une idée...



Il y a quelque temps, Microsoft a sorti Windows Genuine Advantage (WGA pour les intimes), un programme spécifique destiné à lutter contre le piratage le plus néfaste. Programmé pour vérifier si un client ou une petite société effectue des copies illégales de Windows XP, WGA agit en deux étapes : l'authentification WGA, puis la notification. Ce sympathique programme de "protection" de Windows contrôle tout d'abord si tout est conforme aux préceptes du Grand Bill puis, lorsque bien sûr il découvre une infraction, il en réfère à qui de droit (utilisateur de l'ordinateur mais aussi la maison-mère, à Redmond !).

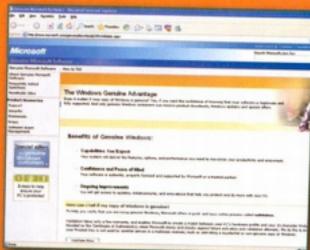
Windows-based existants. La première fois que les utilisateurs effectuent le contrôle d'authentification WGA, les serveurs de Microsoft recueillent les informations suivantes : Windows XP product key, PC Manufacturer, version du système d'exploitation, informations sur le PC BIOS, langue et paramètres locaux de l'utilisateur. Microsoft a chargé la société indépendante allemande TÜV-IT de contrôler la sécurité et la protection des données des utilisateurs, prévues par Windows Genuine Advantage. TÜV-IT a conclu que Microsoft ne traitait aucune donnée susceptible d'être utilisée pour identifier ou contacter l'utilisateur. La société de contrôle a en outre confirmé que Windows Genuine Advantage pouvait être utilisé en toute sécurité dans les systèmes confidentiels, qu'il n'interférerait avec aucun logiciel et que, par conséquent, il n'entraîne en conflit avec aucune réglementation en matière de protection des données.

Bien sûr, on peut facilement comprendre que WGA puisse devenir envahissant : l'idée d'un programme obligatoire qui interroge l'ordinateur sur lequel il est installé, fourre son nez partout, puis en réfère à qui de droit, ne plaît pas forcément à tout le monde et ce, du fait également que WGA fait légèrement office de Big Brother même à l'égard de ceux qui font tout dans les règles... Et alors ?

● L'anti-WGA

Il existe un programme au nom peu orthodoxe, WGA Fucker, qui rend la protection de Windows... bon, allons droit au but, qui la transforme en une véritable passoire.

Le programme est d'un uso simplissime. Ce programme s'utilise très facilement, mais il est tout aussi utile de comprendre son fonctionnement, que ce soit en terme d'interaction avec le système, qu'en terme de programmation en Visual Basic.



▲ Et voici le joli système qui vous trace ! Voyons comment l'enrayer...

Son action peut se résumer en 5 étapes.

Pour commencer, il termine le processus WgaTray.exe qui sans cela ne pourrait être éliminé, dans la mesure où il est utilisé par le système lui-même :

● Juillet 2005 : le tournant !

Depuis l'été 2005, la validation de WGA est devenue obligatoire pour tous les utilisateurs de Windows XP qui tentent de télécharger tout type de programme et patch Windows-related à partir du site de la société. Microsoft a toutefois décidé de laisser la fonction "Mises à jour automatiques" de Windows, libre de tout contrôle d'authenticité en matière de système. Ce choix dérive semble-t-il de la nécessité d'assurer la sécurité générale de l'ensemble des ordinateurs

```
ject ("winmgmts:").ExecQuery("SELECT * FROM Win32_Process WHERE Name='wga tray.exe'")
Obj.Terminate
Next
```

Avec la commande "ShellExecute", on élimine les fichiers responsables du WGA :

```
ShellExecute 0, vbNullString, "du C:\windows\system32\wga tray.exe", vbNullString, vbNullString, 1
ShellExecute 0, vbNullString, "du C:\windows\system32\dlcache.dll", vbNullString, vbNullString, 1
```

Puis, il faut également modifier le registre, en insérant dans le système un fichier .reg avec le contenu suivant (A noter le symbole "-" destiné à supprimer la clé) :

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\wgalogon]
```

Et voici le code qui le copie dans C:\ et lance son exécution. Bien sûr, les méthodes pour interagir avec le registre sont nombreuses, mais nous avons utilisé celle-ci pour faire en sorte que la confirmation effective de l'utilisateur soit demandée au cours du programme pour entrer les informations dans le registre. Le code vb est présenté ici à droite. Vous trouverez une copie du script Visual Basic en exécution automatique, ci-dessous. A noter que l'on pouvait taper Run dans la clé de registre.

```
Dim intfilenumout As Integer
Dim intfilenumout As Integer
Dim outputfile As String
Dim intctr As String
Outputfile = "C:\cancel.reg"
Intfilenumout = FreeFile
Open outputfile For Append As intfilenumout
Intctr = Text2.Text
Print #intfilenumout, intctr;
Close intfilenumout
`etape4
ShellExecute 0, vbNullString, "C:\cancel.reg",
`etape5
```

Le code prévoit également la demande de redémarrage, nécessaire au bon retrait du WGA. Voilà, comme nous l'avons vu, WGA Fucker est très accessible et vous pouvez également l'optimiser rapidement. Attention toutefois : ne commettez rien d'illégal !

```
Dim a As Integer
Dim s As String
Dim d As String
s = "C:\Documents and Settings\All Users\Menu Demarrage\Programmes\
Execution automatique\Scan.vbs"
a = FreeFile
Open s For Append As a
d = Text1.Text
Print #a, d;
Close a
Dom = MsgBox ("Application WGA supprimée avec succès. Pour rendre les modifications effectives,
il est nécessaire de redémarrer. Redémarrer maintenant?", vbYesNo + vbQuestion)
If dom = 6 Then
GetObject("winmgmts:{(Shutdown)}//./root/cimv2").ExecQuery ("select * from Win32_Operatin-
gSystem where Primary=true")
Else
End If
```

Ctrl_alt_canc
 Ctrlaltcanc.8@gmail.com
<http://ctrlaltcancorp.altervista.org>

Impossible d'éradiquer la concurrence ?

ALORS, DISCRÉDITEZ-LA !

Microsoft s'allie à Novell dans sa énième tentative d'évincer Linux. Voici comment et pourquoi s'en méfier...

Depuis toujours, Microsoft n'a qu'un objectif en tête : être le numéro un et abattre toute concurrence.

Un jeu qui lui a plutôt pas mal réussi ! Microsoft compte en effet trois succès à son actif : Windows, Office et enfin Explorer, le succès des deux derniers étant dû au monopole conquis par Windows. Pour le reste, Microsoft a toujours subi des échecs. Que ce soit au niveau des ordinateurs de poche et téléphones portables, ou avec PocketPC alias Windows Mobile, le géant de l'informatique n'a jamais réussi à raffer la première place. De même pour les consoles (non seulement second après Sony, mais désormais troisième derrière Sony et Nintendo). Même refrain pour la musique car personne ne peut ébranler l'iPod, etc., etc.

Grâce à Windows et Office, Microsoft encaisse des millions de dollars et utilise cet argent telle une machine de

guerre pour évincer toute concurrence quel que soit le secteur.

Pour donner ne serait-ce qu'un exemple : la société a vendu tout un tas de Xbox au rabais, uniquement pour faire du tort à la PlayStation. Du temps de la guerre des navigateurs, elle offrait Explorer gratuitement pour mettre à genoux Netscape qui était payant. Et ainsi de suite...

Un mal incurable

Depuis quelque temps, Microsoft a une peur bleue de Linux. Linux fonctionne mieux, il est plus sûr, plus beau et il est gratuit ! Au début, Microsoft a ignoré le problème : Linux était difficile et uniquement destiné aux passionnés d'informatique.

Puis, Linux s'est simplifié et a touché plus de monde, Microsoft a alors commencé à l'insulter. Steve Ballmer, administrateur délégué de Microsoft, a ainsi défini Linux de cancer de la propriété intellectuelle. La société a même publié de fausses études et recherches pour

montrer que Windows était plus efficace que Linux. Mais ça n'a pas marché : les gens ne sont pas dupes et ne tombent pas dans le panneau si facilement. Le nombre de virus, à lui seul, en dit long ! C'est ainsi que Microsoft a dé-

LORSQU'ON PARLE DE FUD

FUD signifie Fear, Uncertainty and Doubt (peur, incertitude, doute). Il s'agit d'une tactique de marketing peu scrupuleuse qui consiste à jeter le trouble sur les produits de la concurrence. C'est IBM qui l'a inventée dès les années 60, lorsqu'elle envoyait ses vendeurs chez les clients pour expliquer que "personne n'avait jamais été licencié pour avoir acheté des produits IBM". Autrement dit : vous voulez acheter quelque chose d'autre ? Si ensuite vous vous faites licencier pour vous être trompés, c'est votre problème ! Aujourd'hui, Microsoft pratique le FUD sans limite. Un exemple : l'accord avec Novell qui sert uniquement à faire peur aux autres.





chez Sun Microsystems, ces sociétés passent des accords et font tourner de l'argent sur une chose qui, en réalité, ne leur appartient pas. Donc, quel est le sens de cet accord ?

::Attention à vos choix...

C'est très simple : faire peur à tous les autres. Microsoft passe un accord avec Novell, intègre Suse à ses futurs produits de virtualisation (du style : tu peux aussi utiliser Linux, à condition que ce soit sous Windows) et dit, en substance, ok, si vous utilisez Suse, on ne vous causera pas d'ennui.

Pour tous les autres, un procès, un boycottage, une campagne de presse, restent de mise. La menace n'est pas tant adressée aux personnes normales qu'aux entreprises. Vous souhaitez vraiment utiliser le cancer Linux ? Utilisez le nôtre, ou sinon on se reverra sans doute au Tribunal, ou Dieu seul sait où !

:: Chien qui aboie ne mord pas, mais effraie quand même

L'ennui, ce n'est pas tant que Microsoft se mette réellement à faire la guerre à tous ceux qui souhaitent adopter Linux. C'est perdu d'avance ! C'est pourquoi, elle cherche à faire peur et à jeter le trouble parmi les administrateurs réseau et dirigeants qui commencent à penser : je peux utiliser Linux mais ce n'est pas le Linux qui plaît à Microsoft, et si ensuite il arrive quelque chose, s'il y a un problème de brevets, un micmac avec les licences... ? C'est exactement ce que souhaite Microsoft : jeter le trouble dans l'esprit de tous ceux qui pourraient peut-être décider de passer à Linux. Plus il semble y avoir de risques, moins les gens auront envie de passer à Linux.

:: Vous avez dit compliqué ?

Certes, il ne s'agit pas d'un accord commercial mais d'une manœuvre tactique (et déloyale), et

QUI VEUT SUSE ?

Allez jeter un œil à la page www.linux.org/dist/list.html. Vous y trouverez une centaine de distributions Linux alternatives, minimum. Avez-vous vraiment besoin de Suse ? La réponse est : bien sûr que non ! Entre Mandriva, Ubuntu, Debian, Knoppix, Red Hat, Gentoo, Slackware... vous n'avez que l'embarras du choix. Et ce sont tous des logiciels libres. 100 % libres !

tout le monde l'aura compris car l'accord est très complexe. Novell elle-même a publié sur son site une page de questions/réponses (<http://snipurl.com/159cp>) qui laisse dubitatif ! Beaucoup de gens se demandent s'il n'y a pas une violation des licences qui protègent la liberté de l'open source, comme la GPL. Principale objection soulevée par de nombreux experts : payer des royalties pour distribuer un logiciel protégé par la Licence GPL, est en réalité impossible (le logiciel peut tout de même être distribué, mais sous une autre licence). Et ce n'est là qu'un point d'une liste d'objections et de problèmes qui n'en finit plus.

:: Ne vous laissez pas bernier !

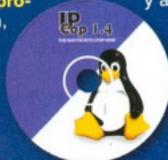
Ignorez les efforts de Microsoft. Comme l'a si bien dit Simon Phipps, Microsoft et Novell s'accordent sur quelque chose qui, en réalité, ne leur appartient pas. Laissons-les à leurs affaires et continuons à installer Linux, plus sûr, plus efficace, plus agréable, plus libre et plus économique ! La guerre de Microsoft contre l'open source et contre Linux finira mal. Pour Microsoft, bien sûr ! Car le logiciel libre restera tel quel, peu importe l'argent qu'ils déboursent. Il y a des choses, mon cher Bill, que votre argent ne peut acheter. Voir vos employés circuler dans vos bureaux avec des écouteurs iPod sur les oreilles, doit certes vous énerver. Mais iPod, c'est mieux ! Linux c'est mieux ! Alors, laissez tomber !

Reed Wright
r33dwright@gmail.com

cidé d'utiliser son flot d'argent pour faire la guerre à un système gratuit. Ainsi va la vie...

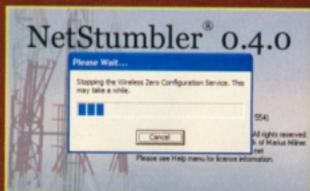
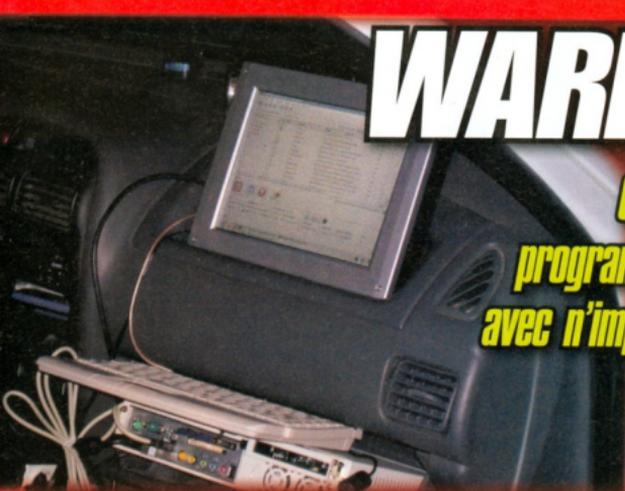
:: Une collaboration de 308 millions de \$

La distribution Linux Suse est la propriété de Novell. Microsoft a passé un accord de 5 ans avec Novell stipulant que les clients Microsoft pourront bénéficier d'un support et d'une maintenance sur Suse Linux Enterprise Server. Microsoft s'engage, quant à elle, à investir plusieurs millions de dollars pour la promotion et le marketing des produits Suse Linux. Enfin, les deux sociétés cesseront tout procès sur des questions de brevets et de technologies actuellement en discussion. Et nous en arrivons au cœur du sujet ! Comme l'a commenté Simon Phipps, grand maître de l'open source



WARDRIVING

Configurez le plus célèbre programme de Wardriving et ce, avec n'importe quelle plate-forme !



▲ Avant modification, avec NetStumbler activé...

Combien de fois avez-vous lancé votre Netstumbler sans parvenir à vous connecter à votre réseau préféré et ce, parce que votre programme de connexion sans fil était tout simplement verrouillé ? Eh bien ! Oui, vous pouvez contourner le problème ! NetStumbler est un excellent program-

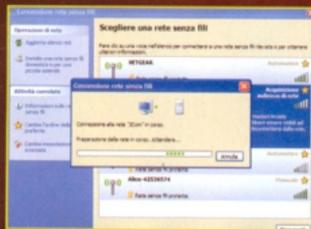
me des fonctions disponibles qui, sans cela, rendrait ce puissant logiciel peu utilisable voire inutile.

Commencez tout d'abord par créer une copie de sauvegarde du programme pour éviter de le perdre définitivement après une modification erronée.

Le truc est très simple ! Le programmeur de NetStumbler a sans doute inséré une instruction "if" qui contrôle l'existence de Microsoft Wireless Zero Configuration, qui fait apparaître lors de son lancement le formulaire de recherche et le verrouillage de ce dernier.

fiant comme il se doit, vous éviterez de lui faire faire le "saut" à la ligne qui lui dit de verrouiller le Wireless Zero Configuration. Autrement dit, c'est ce qu'on appelle dans le jargon informatique, appliquer un patch.

A présent, une fois ce patch créé, en modifiant les jumps du code désassemblé, il ne vous reste plus qu'à comparer les différences du fichier binaire d'origine avec la protection, avec celui "patché"... Plutôt simple, non ?



▲ Ça y est c'est fait ! Tout fonctionne à la perfection, même avec les services Windows

:: A quoi pourrait-elle bien ressembler ?

A un pseudo-code synthétique de ce genre (les API de Windows ont sans doute été utilisées) :

:: Utilisez un éditeur

```
if WindowsAPI.Wirelessconfig = true then
  frmcloseconfig.show
end if
```

Munissez-vous d'un éditeur hexadécimal. Nous, nous avons utilisé Frhed (<http://www.kibria.de/frhed.html>), un logiciel gratuit et open source avec lequel nous avons effectué la modification nécessaire au fonctionnement.

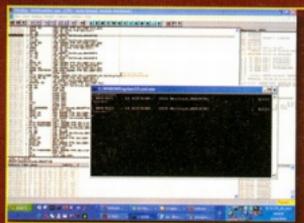
me de détection de réseaux sans fil non sécurisés (et sécurisés), dont vous pouvez bénéficier lors de vos séances de wardriving ou de connexion abusive aux réseaux des voisins. Seule ombre au tableau : ce software ne peut être utilisé avec Microsoft Wireless Zero Configuration (l'outil de connexion sans fil intégré à Windows), sur décision de son programmeur. En tant que hackers avertis, c'est à nous qu'il revient alors de le modifier pour profiter pleinement

Bien sûr il ne s'agit-là que d'un exemple en vue d'être plus explicite ! A présent, en suivant pas à pas le flux du programme par le biais d'un debugger, vous parviendrez à remonter à l'instruction du code assembly qui commande le contrôle. En la modi-

ficant, nous avons utilisé Frhed (<http://www.kibria.de/frhed.html>), un logiciel gratuit et open source avec lequel nous avons effectué la modification nécessaire au fonctionnement. Bien sûr tout autre éditeur hexadécimal fera parfaitement l'affaire. A travers la fonction "rechercher" ren-

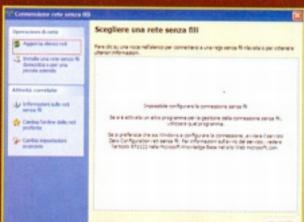
QU'EST-CE QU'UN PATCH ?

On peut lire sur Wikipedia : "La production de logiciels, commerciale ou libre, est habituellement sujette à des erreurs d'écriture du code et à des dysfonctionnements, appelés bogues dans le jargon informatique (bugs en anglais), découverts suite à la distribution du software. Dans son sens premier, patch (littéralement "rustine") est un terme anglais qui, en informatique désigne le hotfix, un fichier exécutable créé pour résoudre une erreur de programmation spécifique, qui empêche le bon fonctionnement d'un programme ou d'un système d'exploitation. Ces fichiers sont généralement délivrés par les fabricants eux-mêmes, en attendant de sortir une nouvelle version du software incriminé". Autrement dit, le patch est une série d'instructions qui ont été modifiées et que l'on peut appliquer comme une macro à des programmes identiques.



▲ Une macro et vous pouvez appliquer les modifications à des exécutables identiques.

par 61 dans la section octets. A présent, allez sur File -> Save As... et choisissez le nom du fichier. N'oubliez pas de paramétrer l'extension manuellement (.exe), afin qu'il ne soit pas enregistré au format texte. Pour vérifier la conformité de toutes ces opérations et éviter toute erreur, voici le checksum MD5 de la version modifiée : 2F753FD1D69B5C4138AEDB572F2 D58FD



▲ Au début, on a l'impression d'être face à un obstacle insurmontable !

Un checksum que vous pouvez obtenir sous Linux avec la commande shell : `md5 [nom programme]` et sous Windows en vous dotant d'un programme quelconque capable d'effectuer une fonction analogue. Vous pouvez à présent diriger l'antenne là où vous captez mieux le signal wireless, en utilisant pleinement NetStumbler.

Ctrl alt canc
<http://ctrlaltcanccorp.altervista.org>
ctrlaltcanc.8@gmail.com

MD5 CA ASSURE !

Pour calculer la somme MD5 d'un fichier sous Windows, à savoir le checksum de toute la suite de bits qui constituent un fichier, il existe de nombreux programmes dont `md5sum` qui, avec seulement 48 ko, vous rendra le service dont vous avez besoin.

Vous pouvez le télécharger sur www.etree.org/md5com.html. Pour les systèmes Windows XP vous pouvez directement le copier dans `c:\winnt\system32`.

Une fois cette opération effectuée, ouvrez la fenêtre de commande (Démarrer -> Exécuter -> `cmd`) et tapez : `md5sum*.ISO>chaînes.txt` ou ce que vous souhaitez : `*.ISO` est le nom d'un ou de plusieurs fichiers que vous souhaitez contrôler et "chaînes.txt", le fichier qui contiendra toutes les chaînes MD5 de chaque fichier contrôlé.

▼ Wardriving : une passion vécue à fond la caisse !

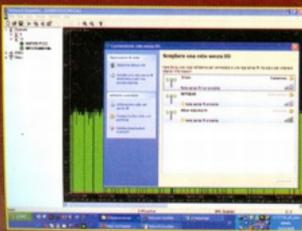
dez-vous à la ligne :

000387b0h

L'éditeur affiche la séquence suivante :

77 7A 63 73 76 63

Modifiez la chaîne comme montré ci-

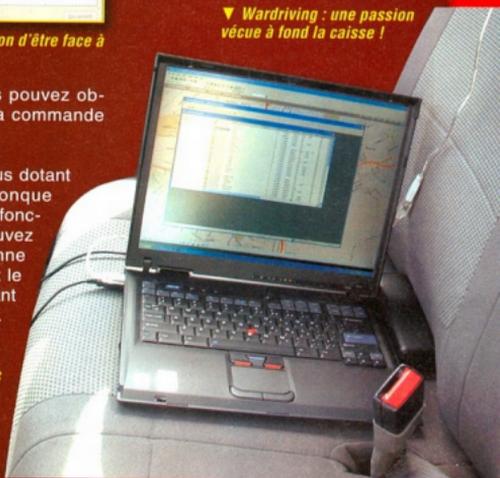


▲ Et après modification ! Toujours avec NetStumbler activé...

dessous : `wzcsvc ----> wacsva`

Ainsi retrouve-t-on dans l'éditeur la modification de la séquence : 77 7A 63 73 76 61.

Nous avons simplement remplacé la lettre "c" par la lettre "a" dans la section alphanumérique, et la valeur 63



Quand votre MESSAGERIE explose !



Voici la solution que vous attendiez tous ! L'adresse "jetable", une nouvelle façon de réduire le nombre de spams et de protéger la confidentialité de votre adresse e-mail

Les occasions de vous retrouver dans la ligne de mire des spammeurs sont vraiment nombreuses, comme lorsque vous vous inscrivez au dernier et tout nouveau service on-line et qu'il

vous est demandé de fournir une adresse e-mail pour contrôler son bon fonctionnement et recevoir un nom d'utilisateur et un mot de passe. Dans certains cas, BugMeNot peut vous venir en aide (<http://www.bugme-not.com>) avec sa grande base de données vous permettant d'accéder en toute liberté à des sites et revues, mais parfois, pas moyen de faire autrement : vous devez obligatoirement fournir une adresse valide et réelle.

De nombreux internautes se sont résignés en se créant une adresse e-mail sacrifiée, destinée à recevoir des ton-

nes de virus, des offres de fausses montres, de médicaments et d'héritages de riches nigériens à racheter. Mais face à cette exigence de fournir une adresse e-mail sans pour autant qu'elle soit prise pour cible, il existe une solution peu connue, mais astucieuse, sûre et très pratique : les comptes de messagerie électronique temporaires.

:: Mode d'emploi

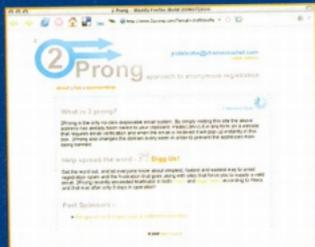
Cette idée de fournir une adresse temporaire n'est pas nouvelle et vous n'avez que l'embaras du choix. Toutes les offres suivent grosso modo le même mécanisme : vous vous créez ou recevez un e-mail flambant neuf généré par le serveur de façon pseudo-aléatoire à utiliser librement, mais qui, au bout d'un certain temps, disparaît tel le carrosse de Cendrillon.

Certains des sites générant ces e-mails temporaires exigent à leur tour votre enregistrement dans leur base de donnée. En échange, ils vous procurent une adresse@leursite d'une durée variable, pouvant aller de quelques heures à quelques jours.

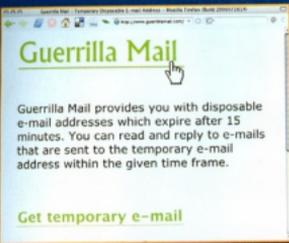
En voici quelques exemples : Spa-

UNE IDÉE CONTAGIEUSE

Le concept d'e-mail temporaire est une idée intéressante qui a fait son chemin et pas mal d'adeptes. La liste de ceux qui peuvent vous fournir une adresse de ce genre comprend des particuliers, associations et même des initiatives commerciales qui se financent par le biais de donations ou de publicités. Pour avoir l'embaras du choix, il vous suffit d'effectuer une recherche sur Google en tapant les termes "disposable e-mail". Pour les flemmards, vous trouverez sur l'URL www.propector.cz/Free-e-mail-accounts/Temporary-e-mail-accounts/, une longue liste (avec des variantes du même concept), claire, constamment mise à jour et dressée par le Tchèque Zdenek Rauner, auquel nous adressons nos plus vifs remerciements.



▲ Les merveilles d'AjAx pour la lutte contre le courrier indésirable : le tout grâce à 2prong.



▲ Pour utiliser Guerrilla, il faut être rapide, très rapide !

mex (www.spamex.com/), Spambox.us (<http://spambox.us/>), Sneakemail (www.sneake-mail.com/) sans oublier Spamgourmet (www.spamgourmet.com), vétéran du secteur. Ce "donnant donnant" est tout à fait facile et compréhensible (surtout par les temps qui courent...), mais assez contradictoire dans la mesure où nous cherchons justement à diffuser le moins possible notre "bonne" adresse et ce, même s'ils nous garantissent qu'ils ne nous enverront aucun spam. Nous nous adresserons donc ailleurs !

:: Prêts ? Feu... Partez !

2Prong (<http://www.2prong.com/>) vous pose en revanche peu de questions et se définit comme "l'e-mail temporaire le plus facile au monde". Pour vous en créer un (qui prendra la forme suivante : mynvqxd6jn@xtremecrochet.com), il suffit de vous rendre sur le site qui vous générera l'adresse et la copiera dans le



▲ Avec Mailinator, nous choisissons nous-mêmes notre e-mail

Bloc-Notes de votre système d'exploitation, à condition que vous ayez un navigateur compatible, comme Firefox. Il vous suffit ensuite de revenir au site ayant fait la demande de l'adresse et de la lui fournir. Cette adresse sera valide tant que vous garderez la fenêtre ou tab de 2prong ouverte. Plus facile à dire qu'à faire !



▲ Spam Gourmet, le site qui mange pour vous tous les spams...

:: En deux temps trois mouvements...

Voici deux sites tout aussi rapides et efficaces : 10 Minute Mail (<http://10minute-mail.com/10Minute-mail/index.html>) vous proposera des adresses e-mails temporaires d'une durée justement de dix minutes tandis que WuzupMail (<http://www.wuzupmail.net/>) vous permettra de les prolonger à trois jours. Avec WuzupMail, vous pourrez choisir votre nom d'utilisateur (par exemple acaro@wuzup.net) et recevoir également le fil RSS des messages. Concernant Guerrilla Mail (www.guerrillamail.com/), son nom parle de lui-même : il suffit d'un clic sur un bouton et une adresse d'une durée de 15 minutes (renouvelables) vous sera fournie. A vous ensuite de l'utiliser comme bon vous semble !

:: Inventez votre e-mail...

Mailinator (www.mailinator.com/) est quant à lui encore plus rapide.

NON, MERCI !

Et lorsque le spam ou le courrier indésirable provient d'un ami ou d'une connaissance ? Dans ce cas, mieux vaut être diplomate et faire gentiment remarquer à votre ami ce qui vous a déplu. Par exemple, avec la lettre ouverte de "Thanks. No" (<http://www.thanksno.com/>) qui fait remarquer à votre connaissance que non, vous n'êtes pas intéressé par la dernière blague, Chaine de Saint-Antoine, avertissement anti-virus ou photo absurde et que vous souhaiteriez que votre adresse ne soit pas visible de tous mais reste privée et à la limite, cachée par le Bcc (Cc en France). Pour l'instant, elle est en Anglais, mais espérons qu'elle sera un jour traduite en Français. Au nom de l'amitié et de nos boîtes e-mail !



Encore un vétéran de l'e-mail qui... disparaît. Avantage de ce site : vous pouvez sauter la phase de création, de demande et de retrait de l'adresse. Vous pouvez vous créer un compte comme vous le souhaitez et lorsque vous en avez besoin (à condition d'être un peu original).

Dans la pratique, il suffit de fournir un nomctif@mailinator.com, puis d'aller sur Mailinator en entrant l'e-mail inventé et d'appuyer sur le bouton "GO" pour lire les messages reçus. Génial, non ? Tellement génial que le procédé a été repris par PookMail (www.pookmail.com/) qui dispose en plus d'une explication et d'une interface en français.

Nicola D'Agostino
www.nicoladagostino.net



▲ Combien d'adresses e-mail allez-vous sacrifier ? Aucune si vous adoptez les adresses "jetables" !

RADIOGRAPHIE du PC

Si quelqu'un sait où chercher, alors fini les secrets ! Découvrez la tanière des fichiers les plus sensibles et la façon dont ils peuvent être débusqués...

Bon nombre de PC vendus aujourd'hui sont souvent des ordinateurs d'occasion. Lorsque c'est le cas, il arrive que le vendeur ait préalablement tenté de supprimer des documents sensibles, en faisant disparaître des e-mails et en vidant le cache des fichiers temporaires sans oublier l'historique d'Internet Explorer, de sorte que personne ne puisse voir les sites qu'il a consultés. A priori tout semble aller pour le mieux ! Tout ce qu'il y avait de compro-

mettant ou de confidentiel a été supprimé ! Malheureusement la réalité est tout autre et de nombreuses informations que l'on ne voudrait surtout pas voir s'ébruiter sont encore là, à portée de clic.

Le registre de Windows

Parfois, le nom d'un fichier suffit à révéler à d'autres personnes, des informations qui devraient absolument rester confidentielles, comme des images et films "particuliers". Ou encore des informations professionnelles personnelles ; si au bureau votre ordinateur laisse une trace d'un fichier "curriculum vitae", votre chef pourrait alors comprendre que vous avez hâte de changer de boulot... Vous pouvez facilement trouver des informations de ce genre dans les menus des documents récents (celui qui se trouve dans le menu Fichier de nombreux programmes). Ces informations sont presque toujours enregistrées dans le Registre de Windows, mais pour les supprimer, il faut savoir où aller chercher. Toutes les applications ne disposent pas nécessairement d'une commande permettant de supprimer définitivement ces informations...

Avant d'aller plus loin, voici un conseil



▲ Inutile de supprimer l'historique des sites visités et de vider le cache : si votre PC finit entre les mains d'une personne malintentionnée, rien ne pourra l'arrêter !

d'ami : le Registre de Windows est très délicat. Si vous mettez les mains là où il ne faut pas, et modifiez un peu trop d'éléments, votre ordinateur pourrait devenir inutilisable. C'est pourquoi, il est important d'effectuer une copie de sauvegarde du Registre (à partir de Regedit, sélectionnez Exporter dans le menu Fichier, assurez-vous que la zone d'exportation soit paramétrée sur "Tout", et enregistrez le fichier dans un lieu sûr), et de copier les fichiers les plus importants.





Windows Media Player

Ouvrez l'Éditeur du Registre de Windows : à partir du menu Démarrer, sélectionnez Exécuter, tapez Regedit et cliquez sur OK.

Une fois l'éditeur ouvert, vous pouvez partir à la recherche des clés incriminées, classées par ordre hiérarchique, un peu comme les fichiers et dossiers dans l'Explorateur.

Commençons par les fichiers récents enregistrés par Media Player. Les informations qui nous intéressent se trouvent dans la clé HKEY_CURRENT_USER<\>Software<\>Microsoft<\>>MediaPlayer<\>Player. Les fichiers récemment ouverts sont enregistrés dans la sous-clé RecentFileList ; sélectionnez les rubriques Fichier0, Fichier1 etc., cliquez sur Suppr. puis, confirmez la suppression.

De même, vous pouvez supprimer les URL des contenus en streaming récemment copiés (sous-clé RecentURLList). Si au bout d'un moment, vous en avez assez de toutes ces opérations, vous pouvez également programmer Media Player pour qu'il n'enregistre plus les fichiers ouverts. Allez sur la clé HKEY_CURRENT_USER<\>Software<\>Microsoft<\>>MediaPlayer<\>Preferences. Si elle n'existe pas déjà, créez une nouvelle valeur binaire appelée AddToMRU (cli-

quez avec le bouton droit dans la partie droite de la fenêtre, Nouvelle/Valeur binaire, et tapez le nom). Double-cliquez, et tapez la valeur 00.

Et avec IE ?

Certaines versions de Windows 98 et Millennium, sans mise à jour d'Internet Explorer 5, enregistrent l'historique et le cache dans des fichiers cachés et invisibles, qui restent sur votre disque et ce, même si vous choisissez de vider le cache et d'effacer l'historique. Lorsque nous disons "caché et invisible", cela signifie qu'il ne s'agit pas d'un fichier normal invisible, qui peut être tranquillement observé et ouvert en paramétrant les bonnes options dans Windows (à partir du menu Afficher d'une fenêtre Windows, sélectionnez Options dossier, puis Afficher et dans les options Fichiers cachés, sélectionnez Afficher tous les fichiers).

Ces fichiers sont en effet totalement invisibles de l'intérieur de l'environnement Windows. Vous pourrez réus-



▲ Supprimer un fichier de votre ordinateur ne signifie pas qu'il soit définitivement effacé... BCWipe peut vous aider !

sir à les voir, les copier ailleurs sur le disque, les ouvrir à partir de Windows, vous faire une frayerie face à ce que vous trouverez et enfin les supprimer définitivement, uniquement si vous savez où les dénicher. Pour plus d'informations, lisez l'encart consacré à IE dans cet article. Les dernières versions de Windows et

MALIN L'EXPLORER !

Certaines versions de Windows et d'Explorer ne suppriment pas les fichiers du cache et de l'historique lorsqu'on agit sur les commandes spécifiques dans Options Internet. Pour savoir si votre système rencontre ce problème, suivez les étapes suivantes :

- 1 - Ouvrez Explorer, allez sur Outils/Options Internet, et à partir de l'onglet Général, cliquez sur les boutons Supprimer fichier dans l'encadré Fichiers temporaires Internet, et Supprimer Historique dans l'encadré Historique. Cliquez sur Appliquer, puis sur OK.
- 2 - Vous devriez avoir supprimé toute trace résiduelle de vos précédentes navigations, exact ? En réalité, pas tout à fait ! En effet, si vous allez sur c:\>Windows<\>Temporary Internet Files, vous verrez que tous les cookies sont encore enregistrés, et qu'ils révèlent presque à coup sûr le site qui les a émis (vous pouvez y accéder également par la fenêtre Options Internet, en cliquant sur le bouton Paramètres dans Fichiers temporaires Internet, puis sur Afficher fichier).
- 3 - Si votre ordinateur n'est pas paramétré ainsi, activez l'affichage de tous les fichiers, même ceux cachés et les fichiers système, comme expliqué ci-dessus. A présent, observez votre dossier de fichiers temporaires (c:\>Windows<\>Temporary Internet Files).
- 4 - Si vous voyez la barre d'adresse dans la fenêtre de Windows, essayez de taper <\>Content.IE5 à la fin de l'adresse affichée. Windows n'affiche aucun message d'erreur. En revanche, il affiche le contenu d'un dossier qui, en théorie, n'existe pas. En l'occurrence, le contenu est une fenêtre blanche, car le dossier est vide. Mais en êtes-vous vraiment sûr ?
- 5 - Essayez d'effectuer un autre ajout au parcours affiché dans la fenêtre. Après <\>Content.IE5, tapez <\>index.dat. Ce fichier, ouvert avec un éditeur de texte, affichera une liste de Url visités. Vous êtes en train de visualiser un fichier qui, selon Windows, n'existe pas... alors soyez attentifs !

BCWIPE

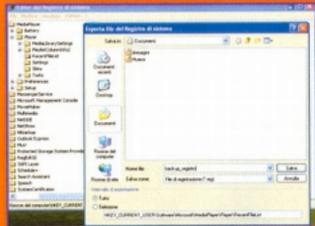
Les utilisateurs ignorent souvent qu'en supprimant simplement un fichier de leur ordinateur, celui-ci n'est pas supprimé définitivement du disque dur. Si vous avez besoin de supprimer totalement certaines données de votre ordinateur, un programme comme BCWipe peut vous être d'un grand secours. Les informations supprimées d'une mémoire de masse de type magnétique restent un certain temps avant d'être effectivement rendues totalement ou partiellement illisibles. BcWipe vient au secours des utilisateurs souhaitant s'assurer de la suppression effective d'un fichier, de façon à ce que personne d'autre ne puisse en aucun cas récupérer les informations supprimées. Le programme s'intègre parfaitement à Windows et à son shell (Windows Explorer), en garantissant une suppression des données selon une procédure des plus rigoureuse et en veillant également au nettoyage de l'espace libre disponible sur une ou plusieurs mémoires de masse. Parmi les fonctions secondaires du programme, rappelons la possibilité de programmer les interventions et celle de supprimer l'espace resté inutilisé au niveau des cluster, dans le cas récurrent d'un fichier n'occupant pas tout l'espace du cluster. BCWipe comprend différents niveaux de suppression jusqu'aux standards imposés par le gouvernement des Etats-Unis. Avec BCWipe, vous pouvez également nettoyer l'espace libre du disque dur. BCWipe est gratuit et se télécharge sur www.jetico.com/download.htm.

proquo. Attention toutefois : cette opération n'a d'effet que sur les adresses tapées (et non pas sur les liens suivis) et ne retire pas l'information de l'historique ou du Cache d'Explorer, laquelle pourrait être récupérée par un agresseur relativement expérimenté.

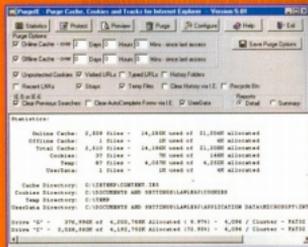
Les fichiers et applications

Windows garde une trace de l'ensemble des fichiers et applications ouvertes par tout utilisateur.

L'affichage de ces éléments dans le menu Démarrer/Documents récents en est l'effet le plus immédiat, mais ces informations pourraient être exploitées de différentes façons. Pour retirer cette fonctionnalité à l'utilisateur actuellement connecté, vous devez vous rendre sur la clé de Registre HKEY_CURRENT_USER<\\>Software<\\>Microsoft<\\>Windows<\\>CurrentVersion<\\>



▲ Le registre est le cœur du système : on ne fait pas une opération à cœur ouvert sans au préalable sauver ce qui peut l'être... Faites un backup !



▲ PurgeE est un programme utile permettant de couvrir toute trace...

Policies<\\>Explorer, créer une nouvelle valeur DWORD appelée NoInstrumentation et lui donner la valeur 1. Pour appliquer cette modification à la totalité du système (et pas seulement à l'utilisateur actuel), faites de même pour la clé HKEY_LOCAL_MACHINE<\\>Software<\\>Microsoft<\\>Windows<\\>CurrentVersion<\\>Policies<\\>Explorer. Pour que cette modification soit prise en compte, redémarrez l'ordinateur (ou reconnectez-vous à l'utilisateur actuel, si la modification n'a été appliquée qu'à ce dernier).

Bien sûr, cette modification pourrait limiter les fonctionnalités de certains programmes ou éléments du système qui doivent accéder à la liste des programmes ou des documents récemment utilisés. Si vous estimez que la modification altère le fonctionnement de certains programmes, vous pouvez supprimer la valeur que vous venez de créer et redémarrer l'ordinateur.

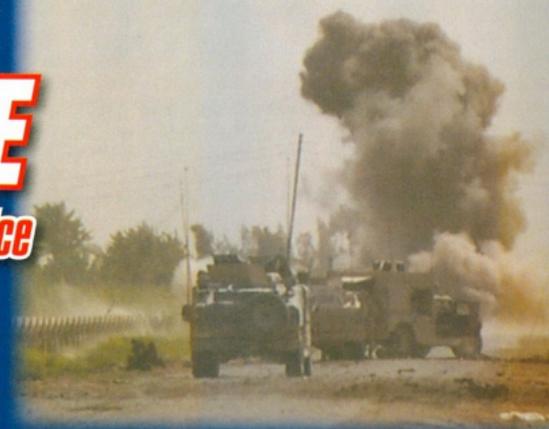
PURGE IE

Un nombre de sites Internet utilisent les fameux Cookies, ces "codes espions" laissés sur votre PC pour enregistrer des informations directement sur le disque dur du navigateur. Pour lire ces cookies, vous devez savoir sous quel nom ils ont été enregistrés (si l'ordinateur de Nicolas utilise un chariot pour réaliser des achats, pour paramétrer un cookie qui rappelle ce qu'il doit acheter, il utilisera "NicolaCart=MB1450, Cyrix200" de façon à rappeler ce qu'il a dans son chariot. Pour lire le cookie, il faut lire spécifiquement le "Chariot Nicolas". PurgeIE est un programme conçu pour aider à garder les cookies et fichiers de cache pour Internet Explorer. Les principaux fichiers INDEX.DAT sont gardés sans qu'il soit nécessaire de les télécharger à nouveau. PurgeIE sert également de "Track Cleaner" pour empêcher d'autres personnes de voir la liste des sites récemment visités. L'option Aperçu permet de montrer le résultat de chaque opération Purge avant son exécution. PurgeIE peut se substituer au "Nettoyage du disque" de Windows et effectuer une suppression plus efficace de cookies, URL visités, fichiers temporaires, données récentes. Il s'agit d'un programme freeware et téléchargeable sur www.purgeie.com/download.htm.

d'Explorer ne connaissent pas ce problème, et suppriment effectivement les fichiers du disque. Quelqu'un pourrait toutefois avoir des soupçons s'il s'aperçoit que la totalité de l'historique est constamment supprimée. Mais vous pouvez faire en sorte que les adresses tapées dans la barre d'Explorer n'apparaissent pas lorsque vous commencez à taper un nouvel URL, sans pour autant supprimer la totalité de l'historique. La clé de registre qui nous intéresse cette fois est la suivante : HKEY_CURRENT_USER<\\>Software<\\>Microsoft<\\>Internet Explorer<\\>TypedURLs. Vous pourrez y voir les adresses tapées dans IE, et supprimer uniquement celles prêtant à qu-

Sniffing MILITAIRE

D'anciens crackers au service du Pentagone utilisent des techniques de sniffing pour neutraliser les bombes.



Le sigle IED signifie **Improvised Explosive Device** : un engin explosif improvisé. Il s'agit de ces terribles engins qui englantent en permanence l'Irak, placés par des insurgés et terroristes le long des routes où passent les convois militaires américains. Il n'est pas question ici des fameuses voitures piégées, ni des terribles auteurs d'attentats suicide, mais de bombes qui sont loin d'être improvisées. Il s'agit de pièges explosifs, souvent enterrés dans le sol à proximité de la route, et constitués d'anciens projectiles d'artillerie ou autres explosifs, reliés à un récepteur radio ou à un téléphone portable. Un signal, un coup de

fil et l'engin explose. Une méthode tristement élaborée qui a fauché de nombreuses victimes. Mais la donne est peut-être sur le point de changer.

Depuis quelque temps, l'armée américaine utilise des véhicules spéciaux, les fameux Stryker, issus des toutes dernières technologies et optimisés pour lutter contre les combattants irakiens et étrangers s'opposant à l'établissement de la paix dans leur pays. Ces stryker sont plus légers et plus maniables que les chars d'assaut. Equipés de caméras de surveillance pour réduire au minimum l'exposition des troupes, ils utilisent depuis peu des techniques de sniffing très évoluées.

munications militaires sont, quant à elles, assurées par l'utilisation de fréquences préétablies "laissées passer" car autorisées.

De l'origine de la découverte

L'origine de cette "nouvelle arme" est terrifiante : il ne s'agit pas de laboratoires de recherche très sophistiqués mais bien d'un groupe d'ex-crackers qui, au cours de ces dernières années, semblent travailler sous des noms de code qui changent tous les 6 mois. Certains disent qu'il s'agit d'anciens détenus, désormais réhabilités dans la mesure où ils ont accepté de travailler pour le Pentagone. D'autres disent en revanche qu'il s'agit de spécialistes indépendants qui ont accepté d'offrir leurs services en exclusivité aux forces armées. Ce qui est sûr, c'est que la technologie à la base de cette pratique rappelle pour beaucoup le sniffing de paquets de données pratiqué par certains "escrocs". Inutile de dire que les Stryker qui parcourent les routes de l'Irak utilisent également des techniques de wardriving spécifiques pour identifier l'origine du signal...

Nous avons raison : la guerre des hackers a commencé. ■

De fins limiers militaires

L'idée est simple : au passage de véhicules militaires spéciaux, toutes les fréquences radio et de téléphones portables sont "sniffées" par des antennes spécifiques placées sur ces Stryker modifiés.

Les véhicules analysent rapidement les signaux transmis et suppriment les signaux d'appel dirigés dans la zone où se trouve le véhicule, en créant une véritable "bulle" dans laquelle tout réseau est supprimé. Cette tactique rend les engins explosifs inefficaces. Les com-



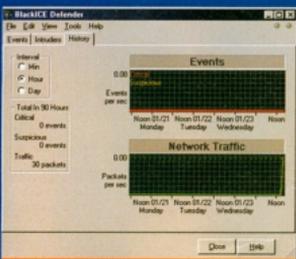
▲ Blindage contre les missiles antichar et capteurs cachés. Les nouveaux véhicules Stryker interceptent les signaux et suppriment les fréquences à l'origine de l'explosion des bombes.

du software de la carte réseau (celui qui gère les MAC address). Les créateurs des Network Based Ids n'étaient autre que les analyseurs de paquets (ou sniffers) tels que Microsoft Network Monitor. Bien sûr, ces applications exigeaient dans tous les cas l'intervention de l'homme pour l'étude du trafic sniffé, empêchant ainsi toute détection d'intrusion opportune. Les applications suivantes, tout en fonctionnant de la même façon, possèdent, quant à elles, des fonctions de reconnaissance de l'activité du réseau, auparavant totalement inexistantes. N'hésitez pas à aller jeter un œil aux spécifications des produits ISS (Internet Security Systems) tels que Real Secure (www.iss).

bles) ou qui contrôlent toutes les opérations de l'administrateur ou encore d'éventuelles tentatives de connexion sur des ports inactifs, etc..



▲ **Un bon IDS peut parfaitement protéger les utilisateurs de tout un réseau, tout en parvenant à notifier à l'administrateur système s'il se produit certains types d'intrusion et en spécifiant l'opération effectuée par l'agresseur et le niveau de risque.**



▲ **Configurez également le niveau d'alerte du programme. Cette option vous permettra de connaître les types d'intrusion ou les éventuelles attaques que votre système subit.**

net/products_services/entreprise_protection/) ou NFR (www.nfr.net). Remarquez que dans le cas présent, nous parlons aussi bien de software que de systèmes hardware.

Host Based Intrusion Detection Systems

Cette catégorie comprend à la fois les analyseurs réseau qui toutefois n'utilisent pas la carte de multiples façons, et n'effectuent donc que la surveillance du trafic destiné à l'ordinateur sur lequel ils sont installés, et les host monitor à savoir ces applications qui contrôlent des activités anormales survenant dans le système, comme des opérations inhabituelles sur le fichier système (la copie d'un fichier de mots de passe et autres opérations sembla-

Pour achever le profil des IDS, citons juste par souci d'exhaustivité les Kernel Based Intrusion Detection Systems, exclusivement programmables sur les systèmes open source. Parmi ces derniers : le LIDS (Linux Intrusion Detection System, www.lids.org) capable de blinder les ordinateurs Linux au niveau des kernels, en empêchant par exemple que l'utilisateur root puisse installer des sniffers.

Place maintenant à quelques IDS simples pour windows, pouvant être utilisés pour protéger votre PC.

BlackICE

BlackICE est un IDS d'Internet Security Systems. Une version d'essai vous est proposée sur www.downloads.com. La version complète coûte dans les 40 dollars. Lors de son installation, le programme crée une liste regroupant les fichiers d'application installés sur votre ordinateur. L'opération demande entre 7 et 20 minutes, selon les performances de votre ordinateur et le nombre d'applications présentes. Une fois l'installation achevée, une icône avec un œil en bas à droite est ajoutée. L'interface d'utilisation est très simple : 4 menus déroulant et trois dossiers. Le premier dossier comprend la liste des événements significatifs survenus. Comme dans tous les event

logger (*journaux d'événements*) qui se respectent, celui de BlackICE permet d'appliquer des filtres en fonction de 4 niveaux de gravité d'événement : informatif, suspect, grave, critique. Pour vous donner une idée de comparaison : un port scan sur votre ordinateur sera interprété comme un événement suspect et la désactivation du BlackICE comme un événement critique. Comme pas mal de Personal IDS actuellement en circulation, BlackICE est équipé d'un pare-feu dont la fenêtre de configuration peut être rappelée à partir de la barre d'outils. Vous pourrez également insérer des règles de filtrage en fonction de l'IP de provenance, du port de destination et du type de paquet (IP, TCP, UDP) et programmer la règle pour qu'elle ait une certaine durée dans le temps. Autre caractéristique intéressante : la possibilité de rappeler la liste des applications créées lors de l'installation et de décider de bloquer une application ou une bibliothèque spécifique, y compris certaines appartenant au système d'exploitation, ou de limiter exclusivement leurs communications vers l'extérieur. Si vous lancez une application absente de la liste, BlackICE vous en avertira et vous demandera si vous souhaitez continuer l'exécution ou non. Dans le second dossier du programme, celui relatif aux intrus, leurs données sont affichées : l'IP de provenance, le Mac address de la carte réseau, le nom NetBIOS identifiant le PC dans son réseau interne, etc..

Quant à la dernière fenêtre, elle est consacrée aux graphiques

► **Si vous ne savez pas qui vous attaque, il n'existe alors aucun outil au monde capable de vous protéger à 100 %.**





▲ Un IDS fournit le même type de service qu'un bon radar de surveillance : il est en mesure d'informer le responsable de la Défense du type d'attaque en cours, garde sous contrôle l'infiltration ennemie et gère au mieux les forces pour intercepter, bloquer et neutraliser l'attaque.

pour vous donner un aperçu immédiat de la situation. Dernière info : à partir du menu paramètres de BlackICE toujours accessible à partir de la barre d'outils, vous pourrez paramétrer les critères de contrôle des applications et de leurs communications avec l'extérieur, ainsi que la façon dont sont enregistrés les logs (également sur fichier ou uniquement sur le journal d'événements) et le niveau de protection du pare-feu intégré.

Les autres Personal IDS

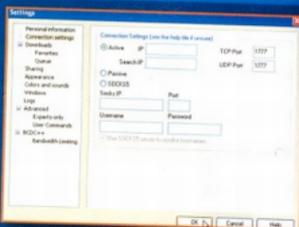
Toujours dans le cadre des personal IDS, le Tiger Guard Personal IDS (www.tigertools.net) mérite d'être si-

gnalé. Même s'il n'a pas été développé par ISS, ce produit reste très efficace tout en étant d'un bon rapport qualité/prix (20 \$). Par rapport au logiciel BlackICE, il ne dispose d'aucun contrôle sur les applications même lorsqu'elles agissent en local. Ce qui n'est pas le cas de BlackICE, et constitue en revanche son point fort dans la mesure où la plupart des Personal IDS ne contrôlent les applications que lorsqu'elles tentent d'accéder à Internet. Un contrôle qui n'est donc pas permanent. Face à cette absence de contrôle, Tiger Guard Personal IDS dispose toutefois d'un sniffer intégré et peut simuler un HoneyPot Server. Il parvient en outre à reconnaître et à bloquer un grand nombre d'attaques (flood, Dos, etc.). A signaler par ailleurs Norton Internet Security de Symantec (www.symantec.com) et Personal Firewall de McAfee (www.mcafee.com).

L'avenir des IDS

La création d'IDS toujours plus performants est cruciale pour la sécurité informatique.

Dans un avenir où de plus en plus d'applications critiques seront mises en réseau (cf. notamment les imminentes réformes sur le e-government), la détection avisée de tentatives d'intrusion ou d'intrusions à proprement parler afin d'éviter ou de limiter les risques, est très importante. Comme pour pas mal



▲ Le pare-feu intégré de BlackICE permet différentes options de paramétrage.

d'autres domaines de programmation, on tente déjà d'appliquer aux IDS les algorithmes typiques de l'intelligence artificielle, en rendant donc les futurs IDS capables d'apprendre à partir des tentatives d'intrusion subies pour parvenir à reconnaître des tentatives d'intrusion absentes de la liste en leur possession.

A cet égard, signa-lons pour les plus courageux, un article de Jeremy Frank du Département Ordinateurs et Sciences de l'Université de Californie, intitulé Artificial Intelligence and Intrusion

Detection : Current and Future Directions, que vous trouverez à l'adresse suivante : <http://citeseer.nj.nec.com/frank94artificial.html>.

RobertodecOder Enea
decoder@hackerjournal.it

► Seules les attaques les plus extrêmes et les plus audacieuses peuvent permettre une intrusion dans un système défendu efficacement par un bon IDS. Mais tout le monde n'est pas en mesure de lancer ce type d'attaques !





Le monde à portée de MAIN...

Réduisez le cumul des données sur les sites pour téléphones portables

A l'heure actuelle, les téléphones portables sont devenus de véritables mini-ordinateurs et ce, grâce au langage WML, conçu pour économiser au maximum de la bande passante. Les templates (modèles) sont l'une des fonctions utilisées : lors-

qu'on envoie plusieurs cartes dans un seul envoi, une template est un fichier contenant un code qui devra être appliqué à chacune des cartes. Mais, au lieu d'être répliqué sur chaque carte, ce code voyage uniquement dans la template. Le téléphone se charge de tout rassembler en lo-

cal, en épargnant un grand nombre de kilooctets. Observez le code ci-dessous. La navigation dépend du code, qui contient un bouton pour se déplacer de la première carte à la seconde et un bouton pour le retour. Le code de la template sera présent dans les deux cartes.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1/EN" "http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
```

```
<!-- Template pour le deck -->
<template>
<do type="prev" name="backbtn" label="back">
<prev/>
</do>
<do type="accept" name="indexbtn" label="index">
<go href="#card2"/>
</do>
</template>
```

```
<!-- Première card dans le deck -->
<card id="card1" title="Ciao!">
<p align="center">
Hacker meme sur les telephones portables!
</p>
</card>
<!-- Seconde card in the deck -->
<card id="card2" title="index">
<p>Cette card est vide</p>
</card>
</wml>
```

échément passer outre le code de la template. Sur-tout lorsque toutes les cartes ont un bouton qui mène à la "home". Cette

opération est appelée shadowing (effet d'ombre) et demande l'utilisation du name (nom) d'un élément. L'élément d'une carte peut prendre le même nom que l'élément dans la template et le premier remplace le second. Voyons maintenant comment désactiver la navigation en arrière dans la carte index. L'élément qui nous intéresse est la commande do, qui a déjà un attribut name (backbtn), c'est pourquoi au niveau de la carte index, il suffit d'intégrer un do+ qui ne fait rien... et suffira à masquer le bouton :

Nous avons la balise <noop/> qui désactive le navigateur. Il doit être compris dans une ancre ou une commande do. L'exemple suivant associe noop à prev :

```
<do name="null" type="prev">
</noop>
</do>
```

Raison de plus d'utiliser un code de ce genre : certains navigateurs pour téléphones portables supportent une fonction back même si elle n'est pas codée dans une page WML.

Reed Wright
r33dwright@gmail.com

:: Astuce

Votre template sera à l'épreuve des bombes mais ne fonctionnera pas bien pour l'une des cartes. Vous pouvez effectuer un override et le cas

```
<carte id="card2" title="index">
<do type="prev" name="backbtn" label="back">
<noop/>
</do>
</card>
```

SKYPE VIA LE TÉLÉPHONE SANS FIL



Téléphoner gratuitement via Skype ? Rien de plus simple ! Mais si vous souhaitez relier un téléphone fixe à votre PC, alors accrochez-vous !

Il ne s'agit pas d'un projet finalisé mais d'une simple ébauche qui s'est traduite par la collecte d'informations sur le réseau, pour apprendre à relier un téléphone sans fil à un PC bénéficiant de Skype.

Ce projet présente deux avantages : Le premier : vous pouvez téléphoner via Skype même si vous êtes dans une autre pièce que celle où se trouve votre PC.

Le second : vous pouvez utiliser votre vieux téléphone sans fil sans avoir besoin d'acheter un téléphone spécifique relié à l'ordinateur via USB. Une solution plus coûteuse, mais qui surtout, ne vous laissera pas libre de vos mouvements.

:: Pourquoi une ébauche ?

Ce projet n'est pas finalisé car il est sûrement perfectible. Relier un téléphone à un PC pour exploiter les capacités de Skype n'est pas aussi simple qu'on pourrait le croire.

Il existe des projets (dont un a déjà été publié) qui exigent l'ouverture et la modification du téléphone, pour brancher

deux fils aux prises casque et micro du PC et qui remplacent donc tout simplement le haut-parleur interne et le micro d'un combiné plus ou moins pratique. Réaliser en revanche un téléphone à proprement parler qui remplace simplement la ligne normale par la connexion à Skype, est une toute autre affaire ! Bien sûr, comme toujours, il existe des solutions commerciales et coûteuses. Mais elles nous font passer l'envie de pratiquer le hacking, qui en revanche nous branche plus que tout !

:: Le problème

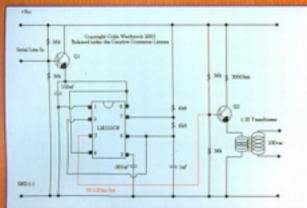
Vous devrez résoudre au moins deux problèmes : construire une interface qui vous permette de relier la base d'un téléphone sans fil à votre PC sans rien modifier, et faire en sorte que lorsque vous composez un numéro sur le clavier du sans fil, celui-ci se transmette à Skype qui déclenchera l'appel.

IMBRIQUEZ TOUT !

Si vous souhaitez accéder à une solution en particulier, vous trouverez sur le web toutes les propositions qui peuvent vous servir. Par exemple, si vous utilisez ce site : http://www.atcom.cn/En_products_AU600.html, vous pourrez passer de Skype à la ligne téléphonique normale uniquement en appuyant sur l'astérisque.

Ce programme pourrait également servir de base pour d'autres mélanges d'interconnexions, comme la connexion sans fil avec un téléphone portable que vous pouvez activer en utilisant Dock-N-Talk (www.phonelabs.com/prd05.asp). Le cas échéant, vous pourrez même devenir un gateway entre VoIP et GSM.





▲ *Internet est toujours une excellente source d'inspiration pour récupérer des ressources et des schémas techniques avec lesquels réaliser notre projet. Pensez-y et au boulot !*

En réalité, il existe également un troisième problème, pour lequel il n'y a pas toujours de solution. Lorsqu'elle existe, elle est en revanche beaucoup plus complexe : faire sonner votre téléphone lorsqu'un appel arrive.

:: Le circuit

Procédons par ordre et commençons par le premier problème : comment faire pour relier un téléphone, quel qu'il soit et sans le démonter, à l'entrée du micro et à la sortie casque de notre carte audio ?

Les solutions présentées ici n'émanent pas totalement de nous, car on les trouve sur le réseau. Celle qui utilise un ré-



▲ *Donnez une nouvelle vie à votre téléphone sans fil, en le reliant à votre PC. Il s'agit d'une procédure intéressante et amusante qui ne demande pas trop de technique.*

seau de découplage entre entrée micro et sortie, est la meilleure que nous ayons trouvée.

La liste des composants :

- 2 fiches jack 1/8" (adaptées aux prises de notre carte audio) ;
- une prise RJ11
- 2 résistances de 150 Ohms 1/2 W
- 1 condensateur électrolytique 1 µF 16 V
- 1 condensateur 0,001 µF 16 V
- une pile de 9 V ou une alimentation 9 V ou encore un câble Usb

Réalisez le montage du réseau de résistances et de condensateurs sur une



▲ *Une réalisation possible de notre circuit.*

plaque à essai, pour trouver la solution la mieux adaptée à votre cas.

Suivez le schéma présenté sur la figure. L'alimentation de la ligne est assurée par la pile (ou un transformateur) 9 volts, ou peut être fournie par une sortie Usb. Dans le second cas, l'alimentation ne sera que de 5 volts, mais la plupart des tests effectués ont montré qu'elle était largement suffisante pour faire fonctionner l'ensemble. Nous préférons toutefois la solution avec pile séparée, dans la mesure où elle n'introduit pas de bruit.



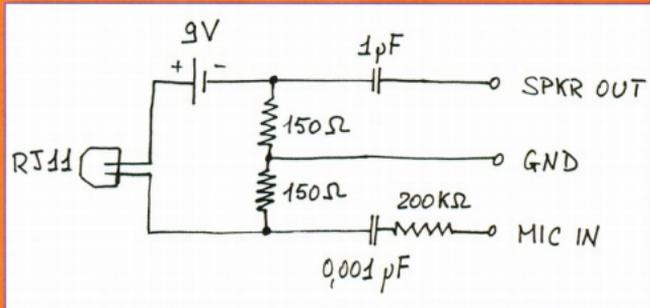
▲ *Tout type de téléphone fera l'affaire pour notre projet.*

Ce circuit présente donc l'avantage de pouvoir être utilisé avec tout type de téléphone, dont vous relierez la fiche à la prise RJ11.

Les sons à l'arrivée et en sortie seront séparés par le réseau de résistances, et les condensateurs éviteront d'introduire une tension continue dangereuse (pour les composants internes) dans la carte audio.

A noter également que certains téléphones ne nécessitent pas d'alimentation. Si vous êtes dans ce cas, vous pourriez alors tenter de supprimer la pile ainsi que les condensateurs, car il n'y a aucun risque à mettre sous tension l'entrée et la sortie de la carte audio.

Pour transmettre à Skype les numéros composés sur le clavier de votre téléphone sans fil, le problème se corse. En effet, Skype n'a pas la capacité d'interpréter les signaux DTMF (dual tone multi frequency) en sortie de votre téléphone. Pour cela, vous avez besoin d'un petit utilitaire. S'il était gratuit et disponible sur le Net il y a enco-



▲ *Suivez les indications de nos schémas et essayez de réaliser un circuit : vous pourrez ainsi redonner vie à votre vieux téléphone sans fil qui languissait dans votre grenier.*



▲ Prêts pour appeler le monde entier, via Skype.

re peu, ce programme pour Windows (et Linux) parfait pour notre projet, est à présent intégré à un package commercial qui comprend une interface très semblable à celle que nous décrivons ici.

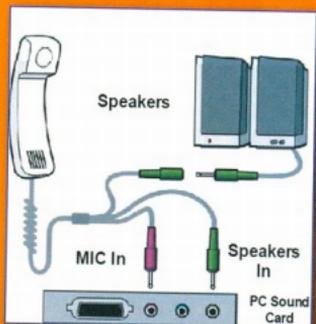
Voici l'adresse : <http://www.chat-cord.com>. Bien sûr, notre esprit de hacker ne s'est pas laissé intimider. Nous avons donc cherché une alternative et en avons même trouvé deux. Vous pouvez ainsi dénicher le même programme sur le site suivant : [http://vital.pr.ee/PSTN/Chat-Cord@DialerXT_v1\[1\].1.0.zip](http://vital.pr.ee/PSTN/Chat-Cord@DialerXT_v1[1].1.0.zip) ou utiliser un autre software, généralement associé à un hardware spécifique, mais laissé sur le Net pour permettre son téléchargement : et

c'est exactement ce que nous avons fait, à l'adresse suivante : <http://phone-converter.com/en/Download.html>. Autre véritable problème restant en suspens : la répétition de la sonnerie. A l'arrivée d'un appel, Skype reproduit le son d'un fichier audio, tandis que n'importe quel téléphone standard a besoin d'un signal alterné de sonnerie de plusieurs dizaines de volts sur la ligne.

Un problème difficile à résoudre.

Nous avons déniché un schéma sur le réseau, même s'il faut le tester (voir l'encart en bas de page). Encore une fois le Net prouve qu'il est une extraordinaire mine d'informations.

Vous devez enregistrer un fichier dans lequel vous associez un signal de 18 KHz à votre sonnerie préférée de Skype. Vous pouvez le construire et le mixer en utilisant Audacity.



▲ Connecter un vieux sans fil à l'ordinateur lui donnera une seconde vie.

La fréquence de 18 KHz, difficilement audible, servira au circuit comme trigger (signal de départ) pour inciter le circuit intégré 555 à produire une fréquence de 50 Hz. Cette fréquence de 9 volts crête à crête est appliquée à un transformateur d'un rapport de 1/40. En sortie, vous pourrez ainsi prélever un peu moins de 100 volts nécessaires pour activer la sonnerie du sans fil.

Les deux transistors montrés sur la figure de ce circuit pour la sonnerie (voir ci-dessous) peuvent être choisis parmi tout type de Darlington NPN : BC517, BC618, TIP100, BC182 feront tous parfaitement l'affaire.

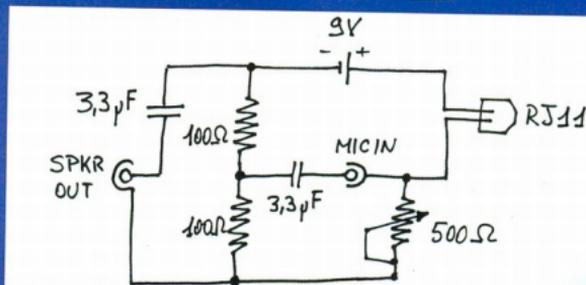
Ce montage est assez difficile, mais c'est la seule solution qui semblerait fonctionner. Ce projet est des plus intéressants car il permet de contourner les limites imposées par des politiques de marché fixées par ces géants de l'informatique qui prétendent nous dire ce que nous devons acheter, utiliser et jeter. Grâce aux solutions présentées ici, votre vieux téléphone sans fil, qui vous a sans doute servi pendant des années, pourra avoir une seconde vie, en devenant un instrument pratique pour communiquer et ce, au nez des préceptes de ceux qui n'ont à coeur que leur propre profit. Mettre au point le projet que nous venons d'illustrer est à la fois amusant et utile : un parfait exercice pour entraîner l'esprit hacker et échapper à un marché "dictateur". Allez, au boulot et gardez l'esprit ouvert quoi qu'il arrive !

Standard Bus
standardbus@gmail.com

UN AUTRE CIRCUIT

Même s'il entraîne peut-être quelques problèmes d'écho supplémentaires, le circuit présenté ici convient mieux à certains téléphones sans fil. Mais vous devrez toutefois tester ce montage. L'achat de quelques résistances vous permettra de choisir la meilleure solution pour votre système.

Bien sûr, vous devrez toujours tester chaque circuit sur une plaque à essai et le réaliser sur une plaque à trous uniquement lorsque vous serez sûr que tout fonctionne parfaitement !



LE COMPLÉMENT INDISPENSABLE

COMMENT DOPER VOS GRAVURES DE DVD

HACKERS

MAGAZINE

Avec
son CD
exclusif

WEBCAM ESPION

Tous les **SECRETS** pour le
CONTRÔLE à distance

FIREFOX
à pleine puissance

BOOSTEZ votre navigateur comme de VRAIS HACKERS !

DANS LE CD ROM 630 MO :

30 PROGRAMMES COMPLETS DONT :
4 POUR CONFIGURER UN SERVEUR DE COURRIER ELECTRONIQUE
12 SCRIPTS PRETS A L'EMPLOI
24 EXTENSIONS DE MOZILLA FIREFOX

REDACTEURS RESPONSABLES : S. S. H. - DIRECTEUR : B. B. H.
TOUT : 800 900 000 - 0000 : 0.000 - 000000 : 00 0000

L 15407 - 17 - P - 4,99 € - 000



EN VENTE DEPUIS LE 28 FÉVRIER 2007



SEPT PATCHS POUR VISTA !

Le système d'exploitation de Windows, cette merveille qui devrait révolutionner la façon de vivre et d'utiliser les ordinateurs dans le monde entier, est enfin arrivé. Superbe, magnifique, flamboyant, plein de nouveautés et... de patches ! Dès sa sortie, Vista a fait l'objet d'au moins 7 patches différents délivrés par la maison-mère.

Pas mal comme lancement inaugural, pas vrai ? Fort heureusement, les problèmes résolus par ces patches ne concernent aucunement la sécurité du système (mais nous savons bien que ce n'est qu'une question de temps, n'est-ce pas ?).

Ces patches sont en réalité de petits "pansements" destinés à combler les failles présentes en matière de compatibilité, performance, stabilité et lancement. Bravo !

Mais autre fait intéressant : Vista a été craqué le jour suivant sa sortie. Ou mieux : son PMP !

Microsoft®

Windows®

que le PMP de Vista empêche la copie de films et de pistes audio protégés, dans ces systèmes disposant de composants non agréés par Microsoft.

Quoi de mieux pour lancer le tout nouveau système d'exploitation sur le marché mondial ? On se serait attendu à mieux d'un système qui a subi une si longue gestation...

Alex Ionescu, un expert canadien en sécurité, a déclaré être parvenu à contourner le PMP intégré de Vista (le Protected Media Path). Monsieur Ionescu soutient