TOUT CE QUE LES AUTRES NOSENT PAS VOUS DIRE

2€
0% DE PUBLICITÉ
LIBERTÉ ET PARTAGE

HACKER news Magazine

LE MAGAZINE 100% SÉCURITÉ LE PLUS LU

CRAKERS DE MSN
ILS VOLENT VOTRE COMPTE

INTERVIEW DE MATT KNOX
HISTOIRE D'UN PROGRAMMATEUR ADWARE

ARP SPOOFING
ESPIONNER UN LAN

DSN EMPOISONNÉS
ATTAQUE SIMPLE ET DANGEUREUSE

HACKING GAMES
TOUS LES BUGS DE PLAYSTATION HOME

Année 6 – n° 26 Bimestriel
mai - juin 2009

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

Les camarades de la rédaction européenne :
Damien Bancal,
BMS, Majo, Gualty.

Traduction et adaptation :
Laurent et Sylvie Arsena

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:
NMPP
Directeur de la publication :
Teresa Carsaniga

Dépôt légal : à parution
ISSN : en cours

Lamer ('lae'mr)
Aspirant cracker, aux capacités et connaissances informatiques limitées, souvent maladroit et disposé à mener des actions douteuses et nuisibles.

Editorial

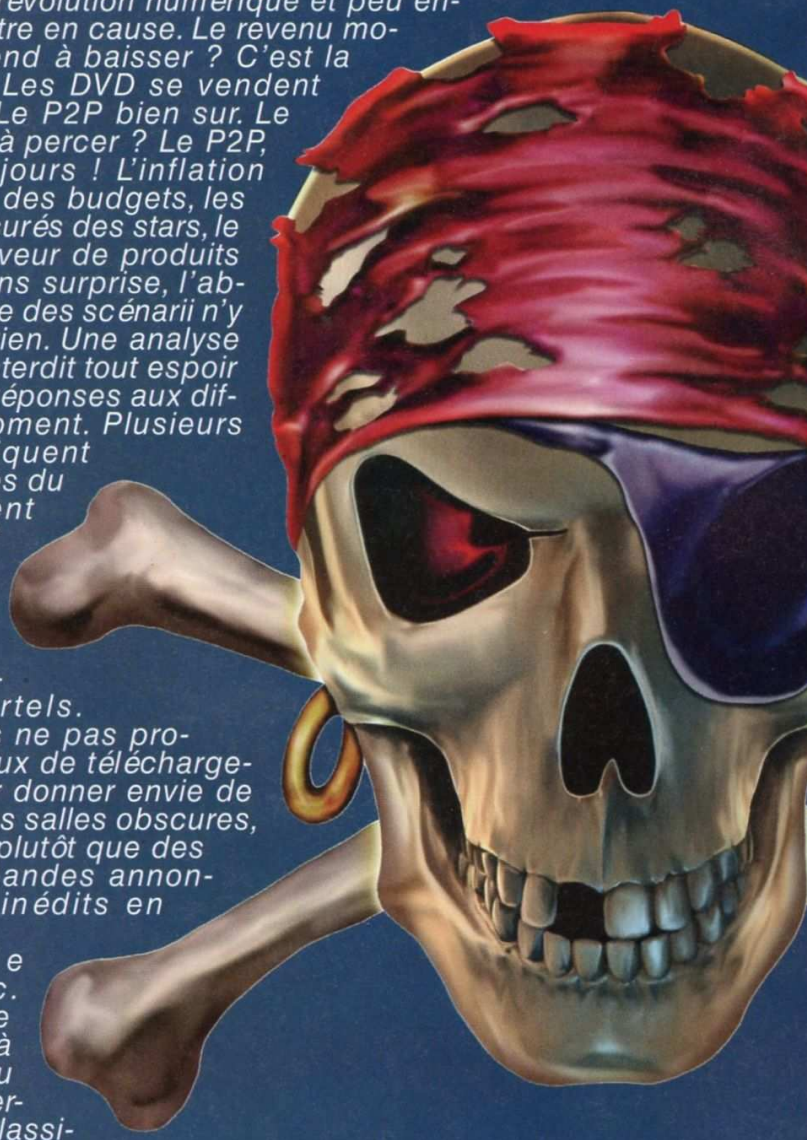
HACKER news Magazine

Et pendant ce temps là...

"La liberté n'offre qu'une chance d'être meilleur, la servitude n'est que la certitude de devenir pire."
Albert Camus (1913-1960)

Cinéma et P2P condamnés à s'entendre ?

La crise tombe bien mal pour un secteur déjà sévèrement secoué par la révolution numérique et peu enclin à se remettre en cause. Le revenu moyen par film tend à baisser ? C'est la faute du P2P. Les DVD se vendent moins bien ? Le P2P bien sur. Le Blu-Ray tarde à percer ? Le P2P, encore et toujours ! L'inflation déraisonnable des budgets, les cachets démesurés des stars, le manque de saveur de produits formatés et sans surprise, l'absence d'audace des scénarii n'y seraient pour rien. Une analyse simpliste qui interdit tout espoir de trouver les réponses aux difficultés du moment. Plusieurs enquêtes indiquent que els adeptes du téléchargement fréquentent davantage les cinémas et achètent plus de DVD que le commun des mortels. Pourquoi alors ne pas profiter des réseaux de téléchargement pour leur donner envie de se ruer dans les salles obscures, en proposant, plutôt que des fakes, moult bandes annonces, extraits inédits en qualité dvd, images de tournage, etc. Pourquoi de pas mettre à disposition du jeune public certains grands classiques, histoire d'entretenir l'amour du 7e art ? Le cinéma est condamné à composer avec Internet. Autant organiser la cohabitation dès à présent.



Distributeur de billets piégé

La police a mis la main sur un distributeur de billets pas sympathique du tout.

La machine, que nous appellerons GAB (Guichet Automatique de Billets), s'était vue gratifiée d'un équipement de skimming. Pour en savoir plus sur cette affaire, voir nos actualités. Voici une démonstration d'une autre "bête" via des photographies réalisées par des cyber-flics Russes.

Notre pirate informatique (35 ans) arrêté dans les Hautes-alpes utilisait quasiment le même matériel. Il a été pris la main dans le sac, ce qui a permis aux policiers de découvrir le matériel à la mode, en ce moment, chez les skimmeurs. Son matériel, un faux lecteur de carte bancaire collé sur le vrai, une mini caméra et un lecteur Arcos 404. Il lui suffisait d'aller chercher son système une fois les clients piégés. Le lecteur copie la bande magnétique. La mini-caméra et le lecteur vidéo enregistraient les mots de passe tapaient par les propriétaires de la carte. L'escroc comparaitra devant le tribunal de Gap, le 11 juin prochain, pour tentative d'escroquerie. Un beau coup pour les forces de l'ordre. Il est rare de tomber sur un matériel encore installé.

En voici un autre exemple. Un distributeur de billets classique. Le pirate a collé un faux plafonnier dans le GAB. Dans ce réceptacle en fer et plastique, des piles, un téléphone portable et une mini caméra. Plus bas, aux niveaux des mains des clients de la banque. Un lecteur pirate de carte bancaire a été posé sur le lecteur officiel. Bilan, la victime rentre sa carte. Elle est d'abord copiée par le procédé pirate puis par le lecteur d'origine. La personne piégée n'a plus qu'à taper son mot de passe au clavier. Ce qu'elle fera en toute confiance et recevra bien son argent.

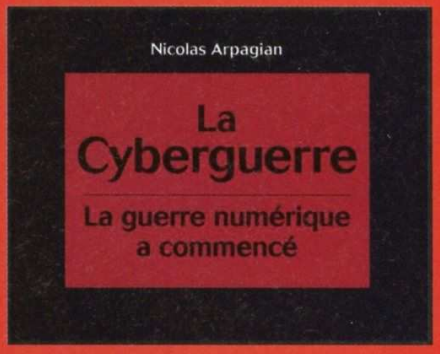
Mais dans un même temps, le pirate aura reçu les données secrètes via un MMS ou un SMS envoyé par le téléphone portable caché dans le faux plafonnier. L'escroc n'a plus qu'à récupérer les informations volées sur les bandes magnétiques des cartes bancaires et à cloner de fausses CB avec les données dérobées. « Ce genre de matériel se vend entre 900 et 4.000 euros, confirme un spécialiste du sujet, Dernièrement j'ai vu du nouveau matériel commercialisé 5 000 dollars. A ce prix, le pirate fourni un mode d'emploi et un logiciel réalisé pour récupérer et traiter les informations volées ». Pas de doute, les pirates ne semblent pas connaître la crise.

NOUVEAUTÉ LOGICIEL

Connu sous le nom de BananaScreen, le logiciel Suisse dédié à la biométrie faciale revient sur le devant de la scène. Il a changé de nom, suite à un problème de nom de marque. Voici la nouvelle monture baptisée KeyLemon qui permet de contrôler l'accès à un ordinateur grâce à son visage. Gilles Florey et Frédéric Favre, co-fondateurs de KeyLemon avaient fait parler d'eux, en 2008. Ils avaient développé des logiciels informatiques basé sur la reconnaissance faciale "dans le but d'augmenter le confort entre ordinateur et machine" indique Gilles Florey. En un an, 400 000 téléchargements, une communauté de 25 000 fans et un retour particulièrement riche de feedback d'utilisateurs. La nouvelle version est encore plus puissante et conviviale dans son utilisation. N'hésitez pas à remonter les failles aux auteurs. http//www.keylemon.com

LECTURE A LA LOUPE

Quarante ans après la création d'Internet, le réseau des réseaux appartient désormais à l'arsenal de tous les États, groupements d'activistes, entreprises ou individus qui contribuent à cette nouvelle forme de conflit où l'information constitue à la fois un support d'action et un actif sensible qu'il convient de maîtriser. La capacité à participer à cette cyberguerre, et à s'en prémunir, est aujourd'hui une des composantes majeures d'une stratégie de sécurité et de puissance pour une collectivité nationale. Cet ouvrage donne les clés pour comprendre les enjeux stratégiques de cet Internet, qui fait partie de notre vie quotidienne. Il explique utilement la manière dont les gouvernements, les multinationales et les militants de tous bords le mettent à contribution pour mener leurs opérations de déstabilisation. Rédigé par un spécialiste des questions d'influence, il rend accessible au plus grand nombre les tenants et les aboutissants de ces cyberguerres qui se déroulent sous les yeux de l'opinion publique mondiale. À lire, pour ne plus rien ignorer de la réalité de ce nouveau visage de la guerre économique, politique et militaire. L'auteur, Nicolas Arpagian est rédacteur en chef de la revue Prospective Stratégique. Coordonnateur des enseignements « Stratégies d'influence & Lobbying » à l'IERSE, auditeur de l'IHEDN et de l'INHES, il est l'auteur de plusieurs ouvrages, tels Pour une stratégie globale de sécurité nationale avec Éric Delbecque (2008, Dalloz) et Liberté, Égalité… Sécurité (2007, Dalloz). Cyberguerre est préfacé par Alain Bauer avec un avant-propos d'Éric Delbecque. (ISBN : 978-2-7117-6893-6) http://www.cyberguerre.eu/

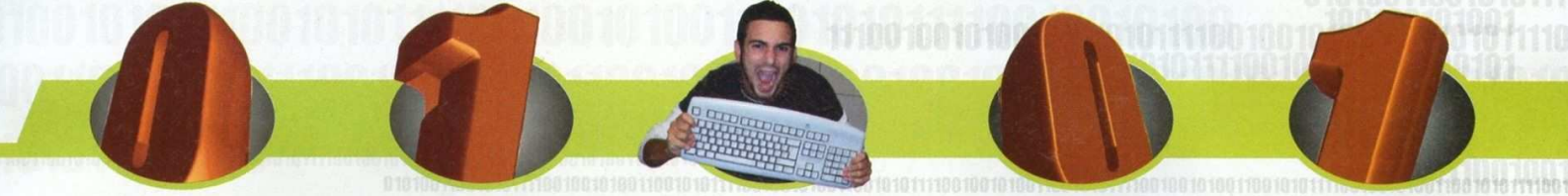


10 SERVEURS DE TORRENTS SAISIS

La police Suédoise a saisi dix serveurs appartenant à Sunnydale, un réseau de partage de fichiers proche de Pirate Bay, en mars dernier. La société, basée à Brandbergen, dans la banlieue de Stockholm, s'est vue amputée de 65 téra-octets de données illégales, soit près de 16 000 films. Le Bureau anti-pirates suédois s'est félicité de l'action au moment ou se concluait le jugement de Pirates Bay. Peter Sunde, l'un des administrateurs de Pirate Bay a indiqué au site SvD.se « Plus de 800 000 personnes ont mis en ligne du contenu sur The Pirate Bay. Donc je ne pense pas que ça soit la source de tout. Mais c'est possible que ça soit une source majeure ».

BUG SUR LE SITE DE CARREFOUR.FR

Mardi 03 mars, 13h30, plusieurs clients découvrent les informations d'autres clients sur leur compte ouvert sur le site Internet officiel de l'enseigne de grande distribution, Carrefour.fr. "Je me suis connecté avec mon compte, indiquait Sylvain sur le site ZATAZ.COM, mais je suis arrivé sur celui d'une autre personne. J'ai recommencé, même pro-



HOT NEWS

INTERDICTION DE SALLE

Louis René Haché, 25 ans, originaire de Montréal a été condamné, le mois dernier, à ne plus mettre les pieds dans un cinéma durant les deux prochaines années. Motif ? Il a été pris la main dans le sac en train de filmer une production cinématographique dans une salle obscure de la chaîne Guzzo. Nous vous parlions de son arrestation qui, au dire de sources proches de l'affaire, s'était plutôt mal passée pour le "camer". En plus de son interdiction de cinéma, il va devoir effectuer 120 heures de travaux communautaires. Autant dire que la peine reste légère. Le Montréalais s'était fait pincer le 26 octobre 2007 au cinéma Guzzo de la rue Lacordaire, à Montréal, lors de la projection du film Dan in Real Life.

PLUS DE 1 MILLION DE MELS EN ACCÈS LIBRE CHEZ HP

Le site officiel du géant de l'informatique Hewlett-Packard (HP) permettait aux spammeurs de fabriquer une petite base de données d'adresses électroniques. Une possibilité que HP n'avait pas prévu dans le code de son site Internet HP.COM. Une base de données de 1 458 511 adresses e-mails aurait pu être confectionnée à bon compte pour les pirates. Un bug idiot dans la protection des données fournies lors de l'inscription à l'une des news letter de HP. La faille permettait de récupérer, à partir d'une page officielle du site, les noms, prénoms et adresses électroniques d'internautes. Il suffisait de changer le dernier chiffre de l'url pour se retrouver avec une identité différente de la sienne. HP a corrigé son problème une heure après avoir été alerté.

165.000 EUROS D'AMENDE

Cinq entreprises canadiennes (Stock-Trak Group, Valcoustics Canada, Capital Engineering, Ion-Ray et Chinook School Division) qui avaient installé des copies dans leurs ordinateurs viennent d'être condamnés à payer 270,000$, soit 165,000 euros de dommages et intérêts à la Business Software Alliance. La BSA est une association financée par Microsoft, Apple, Adobe, Symantec et une cinquantaine d'autres éditeurs de logiciels. C'est la première grosse condamnation au Canada pour des entreprises ainsi contrôlées par la BSA. En 2007, environ le tiers des logiciels installés sur les ordinateurs PC au Canada étaient piratés, selon une étude de l'International Data Corporation pour le compte de la BSA. Les pertes étaient estimées à plus d'un milliard de dollars canadiens, soit plus de 611 millions d'euros.

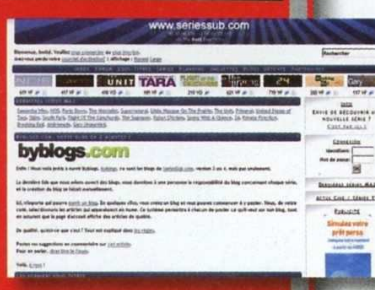
22.000 ordinateurs pirates par la BBC

La démonstration réalisée par la BBC, en mars, dans l'émission Click de Spencer Kelly, a permis de montrer aux téléspectateurs les joies des bots sur Internet. Dans le cadre de son émission informatique, le journaliste a montré comment noyer de millions de publicités non sollicitées des comptes emails ouverts à cet effet. En quelques heures, les boites électroniques ont été inondées par des milliers de messages indésirables (spams). Après la démonstration, la BBC a averti les propriétaires des ordinateurs afin qu'ils corrigent. http://news.bbc.co.uk/1/hi/technology/7938949.stm

blème, sauf que l'identité de la personne avait une nouvelle fois changé." Il n'était pas utile de posséder un compte sur le site Carrefour. Il suffisait sa taper n'importe quel login et mot de passe (comme HNM/HNM) pour accéder à une page client. Le site a été rapidement corrigé.

Sites de sous-titrage de series TV

Plusieurs administrateurs de sites Internet dédiés aux séries TV, des webmasters qui diffusent sur la toile les traductions des séries ont été contactés par le département anti-piraterie du studio Warner. Mission du courriel, faire de la prévention. La missive avait pour mission d'expliquer le danger que posent ses traductions non autorisées "Comme vous le savez certainement, certaines plateformes proposent désormais de manière légale les épisodes de nos séries en version originale avec sous-titres français, parfois même dès le lendemain de leur diffusion aux USA. La diffusion de sous-titres générés par les fans entre en concurrence frontale avec les offres légales qui font leur apparition. D'où la raison de notre demande."

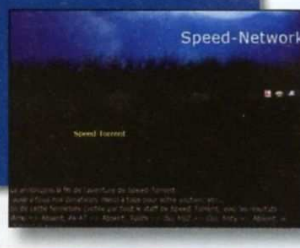


130 000 EUROS À PAYER

Sébastien B. était l'administrateur du site station-divx, un site qui proposait depuis 2006 des informations sur les films sortis en salle comme en DVD. Originalité de son espace web, il offrait aussi la possibilité de trouver des fiches de films (acteurs, date de sortie, synopsis..) avec un lien vers le film payant (via rue du commerce) et une occurrence de mots clés permettant d'affiner les recherches sur eMule. Les indications étaient des occurrences de mots clés du type « titre + langue + format + … » à copier dans eMule. Bien évidement, les majors n'ont pas apprécié cette possibilité de contrefaçon. Bilan, le webmasteur s'est retrouvé devant la justice après une perquisition à son domicile le 18 Juin 2007. Le 5 Mars dernier le verdict est tombé. 130 000 € de dommages et intérêts à partager entre Sony, Vivendi, Paramount, …

SPEED-TORRENT FERMÉ

Une plainte de la SACEM, Le syndicat des auteurs, compositeurs et éditeurs de musique, vient d'obliger les administrateurs du portail Speed-Torrent à plier bagage. La SACEM est un organisme Français qui traite de tout ce qui concerne la déclaration, la protection et la gestion d'œuvre musicale. Les Sept membres fondateurs de Speed-Torrent ont préféré fermer le site de peur de finir avec les gendarmes à la maison "La SACEM a porté plainte (avec preuves) contre Speed-Torrent, explique l'équipe de Speed-Torrent, Les forces de l'ordre ont donc fait leur boulot, nous attendons donc le procès. Nous ne pouvons malheureusement vous en dire plus, et nous avons décidé de fermer toute la partie jugée illégale en France en attendant le PROCES. (...) Nous négocions avec la SACEM afin de pouvoir ouvrir cette future plateforme légalement."



WAREZ ET TRAFIC DE DROGUE, MÊME COMBAT

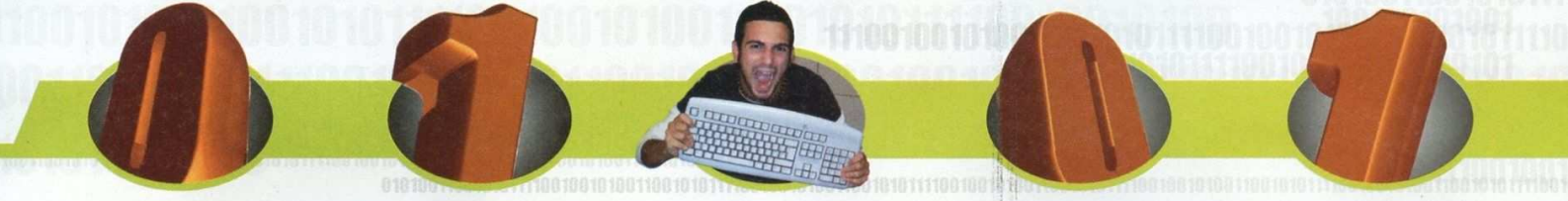
Un rapport de RAND Corporation, une entité américaine, a indiqué dernièrement dans un rapport financé par la MPAA, que les gangs mafieux s'intéressaient de plus en plus au trafic de films piratés. "Une activité lucrative, aux risques faibles" dixit le RAND Corporation. Les mafias du monde rajoutent à leur business le warez en complément du trafic de drogue, du blanchiment d'argent, de l'extorsion ou du trafic d'êtres humains. "Étant donné les énormes marges, il n'est pas surprenant que le crime organisé ait investi le piratage des films" indique Gregory Treverton, coauteur du rapport. Les rapporteurs indiquent ne pas avoir trouvé la preuve de l'utilisation du piratage de films par des groupes terroristes afin de financer leurs actions. "Si vous achetez des DVD piratés, il y a des risques qu'au moins une partie de l'argent aille à des organisations criminelles, et peut-être au terrorisme" conclue le RAND. L'étude a été menée auprès de 120 organisations policière dans plus de 20 pays. "la rentabilité du piratage est trois fois plus élevée que celle de l'héroïne venue d'Iran, et plus importante que celle de la cocaïne Colombienne". indique le rapport.

LEADER PRICE PIRATÉ ?

C'est le magazine professionnel LSA qui a mis la main sur cette nouvelle arnaque. Un site marchand a pris l'apparence de l'enseigne de distribution Leader Price. Ce concurrent pirate s'annonce comme un espace de déstockage de produits high-tech, Leader Price Media (LPM). Il se fait passer pour une filiale des magasins du hard discounter du groupe Casino. Leader Price dément être le propriétaire de LPM. Hébergé aux USA, chez The Planet, la boutique a été mise en place avec l'outil PrestaShop. Étonnamment, l'adresse et le serveur existent depuis septembre 2005. LSA précise que le propriétaire du nom de domaine serait marseillais avec un faux numéro de téléphone. A croire que l'usurpateur lit parfaitement le Français, le 09 mars, ce dernier faisait une modification dans son identifiant Whois et apparaissait comme ... un inconnu qui exploite les services de la société américaine Domains by Proxy, Inc. Une entreprise qui permet de cacher l'identité d'un propriétaire d'un site Internet.

UN AFFLUX DE SPAM RALENTIT TWITTER

Vous vous demandez pourquoi Twitter est devenu si lent ? Un afflux de spam a infiltré la communauté du microblogging. F-Secure a découvert aujourd'hui un compte Twitter frauduleux qui renvoie les utilisateurs vers une escroquerie Google, en promettant un Range Rover gratuit. Un autre exemple est le compte de Kristen Andrew, dont le dernier



HOT NEWS

CODESOFT.CC FERMÉ

Les agents du Landeskriminalamt Baden-Württemberg (LKA), une unité de la police Allemande en charge de la cyber délinquance, ont mis fin aux agissement du forum codesoft.cc. Cet espace était connu pour permettre la mise en relation de pirates spécialisés dans le piratage de données bancaires. Il était aussi possible d'y acquérir chevaux de Troie et autres codes malveillantes. Le forum permettait aussi de mettre la main, contre des euros, sur des "isos" de cartes bancaires piratées à partir de skimmeurs installés sur des distributeurs de billets. Un citoyen Suisse de 22 ans, originaire du Canton de Lucerne, a été arrêté. Il signait ses messages sous le pseudonyme de tr1p0d. Il a été tracé comme étant le créateur et revendeur du logiciel PW Stealer 0.5. Deux autres hommes de 25 et 28 ans ont été arrêtés à Ortenaukrei et en basse Saxe. Ils sont à l'origine de piratage à partir du logiciel espion PW Stealer. Ils sont soupçonnés d'avoir infecté environ 80,000 ordinateurs, depuis septembre 2008, dans le monde entier avec cette application qui permet de voler des mots de passe.

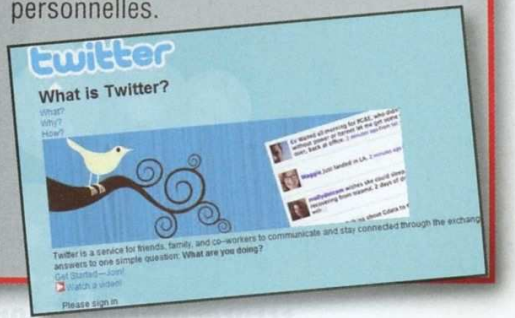
BOULETTE NUMÉRIQUE POUR LE SITE BRAQUEURS.FR

Le site de jeu en ligne Braqueurs.fr a envoyé plus de 20.000 informations sensibles, par courriel, appartenant à ses membres. Une boulette informatique effectuée lors de la demande, par un lecteur de HNM, des récapitulatifs de connexion de ce dernier. Au lieu de recevoir son login et son mot de passe, l'internaute a reçu dans la missive les pseudos, emails, logins et mot de passe des 20.390 membres. Comme l'indique le courrier datait du 5 Mars dernier "Du nouveau sur Braqueurs : Plus rapide, plus élaboré (...) Tous les bugs que l'on pouvait y rencontrer ont au passage été corrigés." Braqueurs.fr est un jeu de Gangsters Virtuels qui offre la possibilité d'organiser des braquages à main armée, vente de matériel sur le marché noir, plantations douteuses, chiens féroces, duels.

SURVEILLANCE DES RESEAUX SOCIAUX

Le ministre de la sécurité intérieure britannique, Vernon Coaker, a expliqué en début de semaine que la conservation des données numériques n'étaient pas assez suffisante. Pour l'homme politique, les réseaux communautaires (Facebook, MySpace, ...) ou de messageries instantanées, comme MSN, devraient aussi être surveillées. Le Ministre Coaker souhaiterai même qu'il soit tout simplement enregistrer. Ils vont se marrer ceux qui vont vouloir "sniffer" ICQ ou encore les Messenger sous SIMP. « Les sites de réseaux sociaux tels que MySpace ne sont pas concernés par cette directive, s'inquiète le Ministre, C'est l'une des raisons pour lesquelles le gouvernement tente de déterminer les solutions à mettre en place dans le cadre du Programme de Modernisation de l'Internet.» Le Royaume-Unis, comme le rappel Vnunet, réfléchit à l'installation de The Big One, la base de données ultime qui doit regrouper SMS, emails, historique de navigation, fax, appels téléphoniques, ... Une base de données consultable par la police mais aussi par les alliés américains du FBI, CIA, ...

Tweet est : « Mon copain m'a envoyé un lien vers un site proposant un concours avec 5000$ à gagner pour le 1er avril, et la participation est gratuite », suivi par une URL. Kristen Andrew prétend vivre à Miami en Floride, et a plus de 1000 suiveurs. Le lien envoie vers une page vous demandant de télécharger le fichier « goldencasino.exe », un jeu de casino. « Twitter est conscient du problème et a supprimé le compte de suiveur de Kristen dans les 10 minutes, mais de nouveaux « scams » (escroquerie via Internet) apparaissent à gauche, à droite et au centre de l'écran », explique Patrick Runald, Chief Security Advisor du laboratoire de sécurité F-Secure. « Les utilisateurs de Twitter doivent vérifier qui les suit, et être attentifs lorsqu'il cliquent sur des URL et des tinyurls. » Le lien promettant un Range Rover gratuit, posté par Jason (Terri962), basé au Nevada, redirige vers une page expliquant comment gagner 5000$ par mois, simplement en postant des liens sur Google. Cliquer sur l'un des liens présents dans ces publicités vous conduit, (après une redirection via krovs.com) vers le site onlinewizards.net où il est expliqué comment gagner 6500$ par mois. Cela semble trop beau pour être vrai ? C'est donc probablement le cas. Pour devenir un annonceur Google Cash on vous demande de donner votre numéro de carte de crédit, et d'autres informations personnelles.



COMMENT Y EST-IL ARRIVÉ

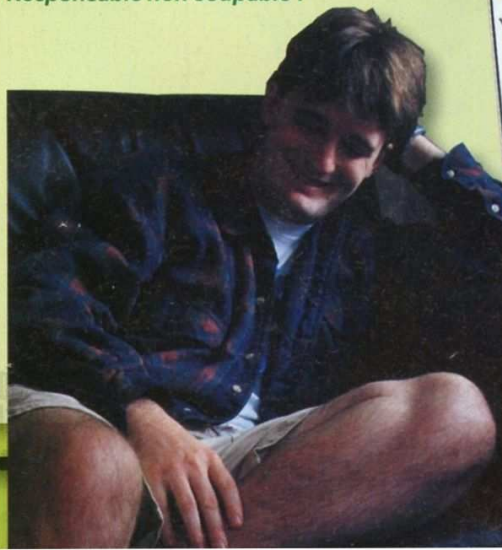
Révélations de Matt Knox, programmeur d'adwares pour Direct Revenue

L'adware ? L'une des plus grandes plaies des internautes : pour pouvoir utiliser gratuitement un programme, nous sommes contraints d'installer le software d'un "partenaire commercial" du développeur. Celui-ci se charge d'examiner votre comportement sur Internet pour cibler vos centres d'intérêt et afficher des banners publicitaires qui vous correspondent. Si certains s'en contentent, d'autres voient cette pratique d'un mauvais œil : pour qui ces espions travaillent-ils et quels types d'information transmettent-ils ? Matt Knox est l'un des programmeurs les plus connus de ce type de softwares. C'est à Philosecurity.org (un blog consacré à la sécurité) qu'il a récemment accordé une interview très intéressante.

:: Pourquoi programmer des adwares ?

Dans son interview, Matt laisse entendre qu'il ne s'agit pas d'un choix personnel : certains programmeurs sont embauchés par une compagnie et se voient attribuer des tâches pouvant également intégrer la création d'adwares. Dans son cas, il ne s'agissait pas au départ d'une demande claire et immédiate : le travail de Matt a été orienté vers un adware plutôt intrusif en partant tout simplement de petites demandes, et en ajoutant peu à peu des demandes de plus en plus spécifiques. Résultat des courses ? Un software qui se comporte non seulement comme un adware tout à fait normal, mais qui est également en mesure de détecter la présence de virus sur le PC empêchant le fonctionnement du programme et de softwares d'autres compagnies concurrentes, afin de les supprimer de l'ordinateur de l'utilisateur naïf. Bref, une guerre menée en sourdine à vos dépens. Et Matt

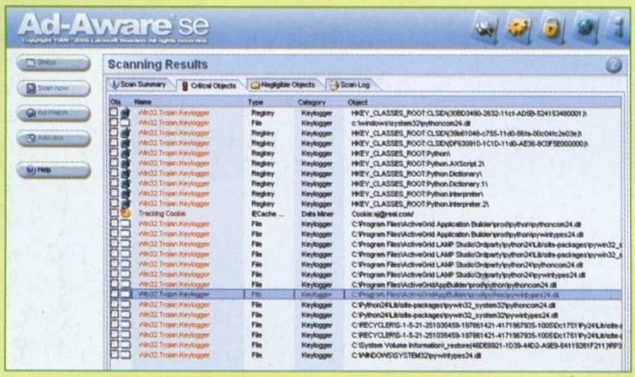
Matt Knox, programmeur adware. Responsable non coupable ?



affirme qu'il est extrêmement facile d'inciter quelqu'un à réaliser une mauvaise action, en la présentant non pas dans son intégralité mais en la morcelant et en la demandant par fragment.

:: L'arrivée sur nos PC ?

Direct Revenue n'appelle pas ça un "adware" : cette compagnie qui s'enrichit grâce à la publicité ciblée, appelle ça un "software supporté par des publicités".
Elle produit un software, par exemple un écran de veille ou un programme utilitaire, puis l'associe à ses fonctions spécifiques. Elle l'offre ensuite gratuitement au public, en échange d'informations sur ses préférences, pour le bombarder ensuite de publicités ciblées. Mais il existe aussi des entreprises "malintentionnées" : ces dernières ne déclarent pas ouvertement que leur programme contient un adware, mais exploitent des failles de sécurité de Windows pour l'installer à l'insu de l'utilisateur. Pour la défense de Direct Revenue, Matt explique qu'une telle conduite n'a jamais été adoptée par sa société : au contraire, dès qu'elle trouvait de tels exploits après analyse des softwares de ses partenaires, elle résiliait le contrat sur-le-champ. Un point litigieux demeure toutefois : ces softwares ont tendance à rester installés même après avoir retiré l'application principale et ce, selon un principe que leurs développeurs nomment "persistence of installation". L'adware continue en effet d'accomplir sa tâche même en désinstallant le programme avec lequel il a été distribué, et fait en sorte de se réinstaller chaque fois qu'un antivirus retire ses composants. Impossible donc, pour un utilisateur normal, de se libérer du software indésirable, à moins de suivre une procédure complexe qui implique de consulter un site Web spécifique, de répondre à un formulaire demandant les motifs pour lesquels vous souhaitez retirer l'adware et de télécharger enfin un programme spécifique qui le retire effectivement. L'ennui, c'est que pour éviter qu'il s'installe à nouveau sur une machine d'où il a été retiré, l'adware entre une clé de registre spécifique, souvent retirée par les antivirus. Le résultat, c'est qu'à court terme, vous risquez à nouveau "l'infection".



Le célèbre programme anti-adware AdAware de Llavasoft. Tout retirer n'est pas toujours la solution...

L'adware exploite des failles du navigateur pour afficher des annonces publicitaires e même lorsque vous faites autre chose

:: Ils se cachent

Tout d'abord, il faut dire que la plupart des adwares frappent Internet Explorer, pour deux raisons fondamentales. Premièrement, les utilisateurs d'IE constituent à eux seuls la majeure partie du marché ; il s'agit habituellement des utilisateurs les moins avisés ou qui ne connaissent pas leur PC, et ignorent qu'IE est affecté de mille problèmes et autres failles de sécurité. Matt a justement utilisé l'une de ces faiblesses : en exploitant le Browser Helper Object d'IE, son adware s'assure que tout va bien en interrogeant la machine toutes les 10 secondes environ. Si un élément manque, il l'installe à nouveau. Avec l'aide d'un petit programme d'installation, les choses deviennent plus simples : on peut écrire des clés de registre pour contrôler la présence des processus souhaités et les réinstaller le cas échéant, et on peut déposer un petit exécutable. Cet exécutable est caché de façon très ingénieuse : on prend l'adresse MAC de la carte réseau, on l'encode avec DEC, on prend les six ou huit premiers caractères et on les utilise pour le nom du fichier. Il existe ainsi un exécutable pour chaque ordinateur, difficile à localiser et ce, même s'il est toujours enregistré au même endroit. La signature MD5 du fichier reste également la même. Le programme est quelque peu "mélangé" : on prend les fonctions incluses et on les enregistre à d'autres endroits que le fichier, en le maintenant exécutable. Les signatures du software sont elles aussi modifiées. Impossible donc de le localiser avec un antivirus ou un programme similaire.

:: Repenti ?

Ce n'est pas la faute de Matt ni des autres programmeurs si aujourd'hui l'adware est une pratique aussi répandue pour diffuser des publicités ciblées, mais plutôt celle des sociétés qui les paient. Qui plus est, Matt affirme que le nombre de fois où son software a retiré virus et autres adwares est largement supérieur au nombre de fois où son software s'est installé, en se présentant ainsi comme un "bon samaritain". Ce qui est sûr, c'est que Matt est dans tous les cas un programmeur honnête et transparent, outre le fait d'être brillant, et qu'il nous a donné l'occasion de mieux connaître le mystérieux fonctionnement d'un adware.

Récupération totale

Si un disque d'un RAID se casse, la récupération des données est facile. Si le contrôleur se casse, cela devient compliqué.

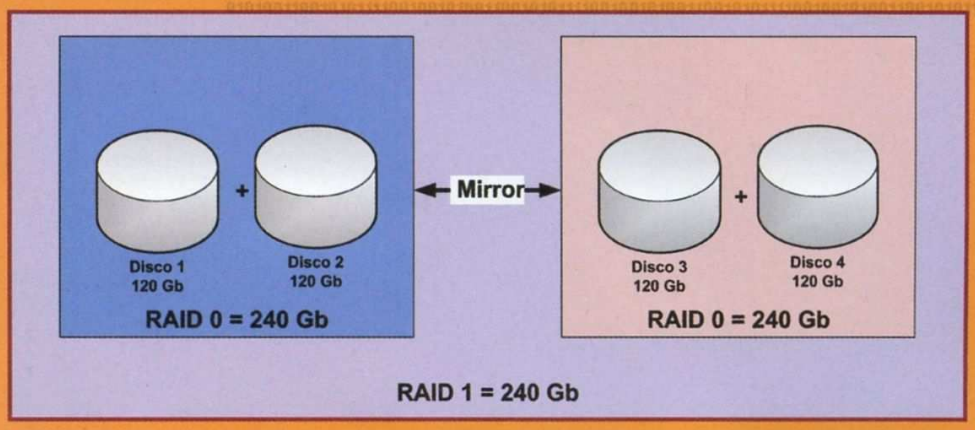
Une architecture RAID peut être définie comme un ensemble de disques physiques qui se comportent comme un seul et unique disque logique. Une technologie utilisée pour les motifs les plus divers : renforcer la fiabilité d'un ordinateur, augmenter la vitesse de lecture ou d'écriture du disque, associer plusieurs disques de faible capacité à travers un disque logique volumineux, etc. A chacune de ces géométries, équivaut un niveau standard de RAID qui va de zéro, pour deux disques ou plus réunis pour en former un seul et unique sans redondance, jusqu'à sept, avec plusieurs disques caractérisés par des systèmes de tolérance face à la rupture d'un ou plusieurs disques, sans oublier un cache en lecture qui améliore leurs performances. Pour se prémunir contre toute panne affectant un disque, on a généralement recours à un RAID de niveau 5 ou, dans des cas de moindre importance, à un RAID de niveau 4 ou 6. D'autres fois, la redondance est obtenue en appliquant plusieurs niveaux de RAID simultanément, comme dans le cas des RAID 1+0 et 0+1, en sacrifiant plusieurs disques pour garder en miroir les unités, en augmentant ainsi les possibilités de récupération.

:: Point faible

Toute géométrie a son talon d'achille, à savoir le contrôleur RAID et les diverses implémentations des développeurs. De nombreux développeurs réalisent des systèmes RAID équivalents avec toutefois une façon propre à chacun de répartir les données entre les disques. A l'exception des simples miroirs (RAID 1), en retirant les disques RAID d'un système et en les mettant sur celui d'un autre développeur, l'architecture RAID ne fonctionne plus. Dans certains cas, il n'est même plus possible de la reconstituer à l'aide des programmes standards. En environnement serveur, où les RAID sont connus depuis longtemps, ces cas sont tout à fait marginaux : il est très rare que la rupture d'un contrôleur RAID entraîne ce type de problème. Dans la plupart des cas, le contrôleur RAID n'est rien d'autre qu'une petite carte ajoutée à la carte mère qui est remplacée par une autre identique. Il ne peut donc connaître de problèmes de ce type.

Avec la diffusion des RAID en environnement domestique, la situation est toute autre : l'intégration du contrôleur RAID dans les cartes-mères, l'évolution technologique permanente, la sortie de cartes-mères toujours plus performantes et la présence sur le marché de nombreux concurrents, compliquent la récupération d'un RAID en cas de problèmes sur la carte-mère avec laquelle il a été créé. Si en théorie il suffit de remplacer la carte-mère endommagée par une autre identique, la récupération d'une carte-mère identique, même si elle provient du même fabricant, est souvent vouée à

l'échec. On assiste ainsi à une situation pour le moins paradoxale, où la rupture d'un composant électronique de la carte-mère empêche l'accès à une architecture RAID où les données sont intègres, tandis que son remplacement par une carte-mère similaire, mais avec une implémentation ne serait-ce que partiellement différente du RAID, ne permet pas d'accéder aux données. Dans tous ces cas, une seule chose à faire : se résigner et formater les disques, en perdant leur contenu, ou bien tenter de reconstituer l'architecture RAID à l'aide d'autres d'outils.



Les RAID 1-0 sont les plus répandus en environnement serveur : ils allient vitesse et capacité du RAID 0 à la sécurité et aux possibilités de récupération des données typiques du RAID 1.

:: Rends-moi mes données !

L'un des outils les plus fiables qui permet, même à des débutants, de récupérer leurs données, n'est autre que GetDataBack, disponible en deux versions, pour FAT et NTFS et produit par Runtime Software, www.runtime.org. Son fonctionnement est basé sur une analyse complète de la surface des disques concernés, en ignorant les fonctions du contrôleur auquel ils sont reliés. La reconstitution est donc logique, en faisant abstraction tant du type de RAID d'origine que du contrôleur auquel les disques sont actuellement associés. Cela signifie qu'il est possible de prendre 2 disques en RAID 0, de les associer à un contrôleur n'ayant aucune fonction RAID et de reconstituer le disque logique équivalent, même si le système d'exploitation les considérera comme des disques vides. Autre caractéristique de GetDataBack : la possibilité d'ignorer toute information du système sur les fichiers, et de se fier uniquement aux données physiquement écrites : idéal pour récupérer les données supprimées accidentellement. En allant au-delà des paramètres de base, ce programme se transforme en un outil très puissant de récupération des données. On vous demande avant tout d'indiquer le problème que vous souhaitez résoudre : récupération de fichiers supprimés, erreur de formatage, destruction étendue des données, comme dans le cas d'une réinstallation d'un système d'exploitation, etc. Vous pouvez laisser tels quels les paramètres par défaut, qui effectuent toutes les analyses de façon approfondie, même si le délai s'allonge en conséquence. Dans l'étape suivante, vous allez devoir sélectionner les disques concernés par le problème. Dans le cas d'un RAID avec plusieurs disques, peu importe l'ordre dans lequel vous les sélectionnez : le programme les analyse et reconnaît à lui seul la structure RAID utilisée.

L'étape suivante analyse les disques et identifie les fichiers système présents : GetDataBack vous fournira une liste des fichiers système qu'il est possible de récupérer, avec leurs caractéristiques. Choisissez celui qui vous intéresse. Vous verrez s'afficher une fenêtre similaire à celle d'Internet Explorer, avec la liste des fichiers et des dossiers présents sur le disque, sans oublier certaines indications des caractéristiques des données : fichiers cachés, supprimés, compressés etc. Vous aurez ainsi la possibilité de les récupérer en tout ou partie, en les copiant tout simplement sur un autre disque, même réseau. GetDataBack fonctionne de façon si linéaire que l'opération qu'il effectue pourrait presque paraître banale, mais ne vous laissez pas tromper : l'analyse lancée sur les disques s'avère parfois très complexe, et les délais peuvent s'allonger, jusqu'à 1 heure par Gigaoctet à récupérer.

L'ARCHITECTURE RAID

Il existe de nombreuses architectures de systèmes RAID, même si l'on en dénombre généralement 5 : RAID 0, JBOD, RAID 1, RAID 5, RAID 10. Concernant le **RAID 0**, deux disques ou plus sont réunis en une seule et unique unité logique, et les données sont morcelées en blocs écrits sur tous les disques. Pour un fichier composé de blocs et un RAID 0 composé de deux disques, la situation typique est la suivante : le bloc 1 est écrit sur le disque 1, le bloc 2 sur le disque 2, le bloc 3 sur le disque 1 et ainsi de suite. Principal avantage : la vitesse d'écriture et la réduction des disques logiques dans le système. Le problème c'est que sa fiabilité est inversement proportionnelle au nombre de disques impliqués dans le RAID. Similaire au RAID 0, le **JBOD** prévoit un enchaînement de plusieurs disques sur une seule et unique unité logique. La vitesse de lecture et d'écriture ne varie pas par rapport aux caractéristiques physiques des disques qui le composent, mais en cas de panne sur un disque, la perte se limite aux données qu'il contient et non à l'ensemble du disque logique. Le **RAID 1** est également appelé miroir et prévoit l'écriture simultanée sur deux disques ou plus avec les mêmes données. L'inconvénient est lié à la perte d'espace. Mais le gros avantage, c'est que la panne d'un disque n'influe pas sur le système. Contrairement aux systèmes vus jusqu'à présent, le **RAID 5** exige au moins 3 disques pour fonctionner. Les données sont écrites sur deux disques, comme c'est le cas pour le RAID 0, tandis que des informations de parité sont écrites sur un troisième disque. Grâce au contrôle de parité, il est ainsi possible de reconstituer les données perdues suite à une éventuelle panne sur un disque. Le **RAID 10** est en réalité une combinaison de RAID 1 et de RAID 0, et exige au moins 4 disques : ceux-ci sont reliés deux à deux dans RAID 1, tandis que les blocs sont associé dans RAID 0.

Mise à nu du réseau social qui fait tourner la tête aux Français

TOUS LES HACKS DE FACEBOOK

Parfois, il suffit d'un mot : Facebook. Et voilà que tout un univers online s'ouvre à soi. Un réseau social qui regroupe à lui seul plus de 160 millions d'utilisateurs. Et qui pèserait plus de 16 milliards de dollars, d'après les dernières estimations. Notoriété, utilisateurs, argent..., tous les ingrédients semblent réunis pour faire un véritable tabac ! Certains détracteurs estiment pourtant que l'évolution de la structure software de ce système ne va pas de pair avec sa célébrité. Des histoires de "bévues" apparaissent ainsi, ayant coûté la sécurité des données personnelles de centaines de milliers de profils. Mais dans le cas présent, nul besoin d'utiliser des techniques de hacker farfelues : il suffit juste d'un peu d'ingénierie sociale. On crée un faux profil, en utilisant sans doute le nom d'un personnage célèbre (pas trop quand même), et on demande à faire partie du "réseau" d'amis d'un utilisateur. Puis, on consacre quelques semaines à observer ses habitudes, grâce aux messages qu'il édite et reçoit. Le poisson a mordu à l'hameçon : on commence alors à communiquer en déviant clairement sur sa vie privée et en obtenant ainsi toutes les informations souhaitées.

Facebook a été créé en 2004 par un jeune de dix-neuf ans, Mark Zuckerberg, actuellement Administrateur Délégué

:: A vous les albums !

Mais le hacking de Facebook ne doit pas être uniquement considéré d'un point de vue négatif. La structure paléolithique du software qui le gère, se prête en effet à de nombreuses optimisations faciles à mettre en place. L'une des plus amusantes ? Celle qui permet de regarder un album photo même s'il appartient à un utilisateur qui ne fait pas partie de votre réseau. Ceux qui connaissent Facebook savent en effet que si un ami est "taggé"

dans l'album d'un utilisateur connu, il leur est alors impossible de voir les autres photos de l'album. Le script "Facebook View Photo in Album", disponible sur http://userscripts.org/scripts/show/9580, vous permettra en revanche d'activer la commande "See this photo in its album". Vous aurez ainsi accès à toutes les photos de cet album. Si l'un de vos amis a choisi en revanche de limiter l'accès à ses albums photos, le script "View All Photos" (http://userscripts.org/scripts/show/11218) vous sera alors d'un grand secours. Il est si puissant qu'il peut réduire à néant d'éventuels paramètres de confidentialité relatifs aux photos, en vous donnant libre accès aux albums. Certes, il ne fonctionne pas à tous les coups, mais vaut la peine d'être essayé.

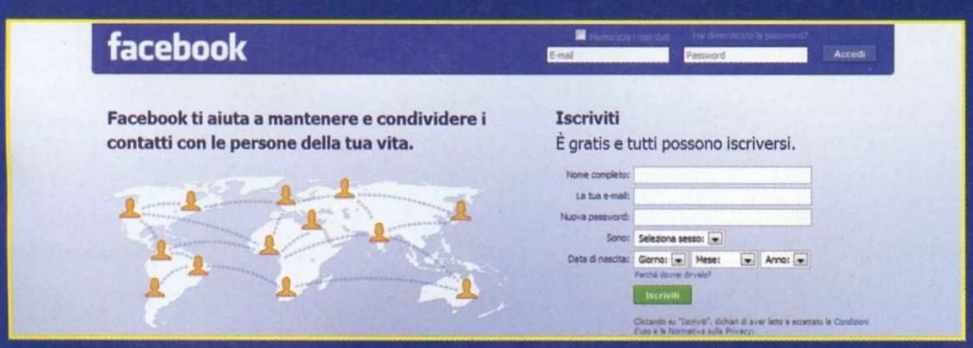
:: Du général au particulier

"FB People Redirect" est en revanche un script qui vous permettra d'afficher le profil détaillé d'un utilisateur dont vous ne connaissez que la page Facebook. A l'instar des services comme LinkedIn. Un utilisateur Facebook dispose en effet de deux types de profil : un profil public, qui généralement apparaît aussi sur Google, et un profil plus complet auquel seules les personnes inscrites au réseau peuvent accéder. Grâce au script "FB People Redirect" (http://userscripts.org/scripts/show/27011), vous pourrez également afficher ce second profil. Nous vous conseillons toutefois d'activer ce script uniquement après vous être authentifié sur Facebook. Dans le cas contraire, vous risquez de provoquer un "loop" amenant tout droit au crash de votre navigateur. Face à ces quelques hacks destinés à saboter quelque peu la confidentialité des données, en voici un qui protégera en revanche la vôtre. Il s'agit de Private Wall (http://www.facebook.com/applications/Private_Wall/20221093560), une application Facebook, encore méconnue de nombreuses personnes, qui protège votre "mur" privé des regards indiscrets. Généralement, les messages publiés sur votre mur virtuel Facebook, peuvent être lus par les personnes inscrites à votre réseau. Ce qui n'est pas toujours agréable en soi, surtout question "anonymat". "Private Wall" rend en revanche cet espace inaccessible et ce, sans toucher aux paramètres de confidentialité des données de votre compte Facebook.

L'un des hacking les plus connus de FB se base sur l'ingénierie sociale : faites-vous passer pour quelqu'un de célèbre et "crédible"

:: Publicité ? Non, merci !

Question confidentialité des données, ajoutons que les nombreux messages publicitaires affichés sur Facebook ont également tendance à lui nuire. Pour les supprimer d'un seul coup, il existe un script au nom très éloquent : Remove All Facebook Ads (http://userscripts.org/scripts/show/13787). Soyez dans tous les cas toujours vigilant quant à la sortie de nouvelles versions qui contournent les solutions trouvées au fur et à mesure par Facebook, pour afficher coûte que coûte les publicités. Par contre, si c'est la publicité qui vous intéresse, en tant que business, Facebook Advertising (http://www.facebook.com/advertising/) est l'application qu'il vous faut ! Il s'agit en effet d'un éditeur de publicités très puissant pour Facebook qui, outre le fait de permettre leur création rapide et complète, garde une trace de ses destinataires. Facebook Refresh 2 Alpha (http://userscripts.org/scripts/show/24225) est quant à lui un script qui actualise Facebook toutes les 30 secondes. Ceux qui utilisent souvent ce réseau social apprécieront, en revanche, la valeur ajoutée d'un script qui double leur "productivité". Refresh Alpha 2 se charge de mettre à jour le feed des news, les notifications et le nombre de messages reçus. Sa nouvelle version sortira prochainement et se chargera également d'actualiser les messages et posts sur les murs. S'il vous est impossible de toujours rester connecté à ce réseau social, une application "officielle" comme FbQuick vous sera alors très utile. Un software qui vous notifie directement sur votre bureau tous les types de messages concernant Facebook, des "demandes" aux messages, en passant par les posts sur les "murs", "pokes" et autres invitations. Vous pouvez le télécharger directement à partir de son site officiel : www.fbquick.com.



La plupart des hacks de Facebook exigent une authentification. C'est pourquoi, vous avez tout intérêt à commencer par vous créer un profil, même s'il est faux, et à vous loguer

Vous n'aimez pas les changements apportés à l'interface des nouvelles versions de Facebook ? Vous pouvez les annuler, en utilisant le script Undo New Facebook Redesign (http://userscripts.org/scripts/show/8482). Un script qui vous permettra d'appliquer "l'undo" aux nouveaux éléments de l'interface.

ADOBE OUVRE LA CAGE

Adobe publie les caractéristiques de Real-Time Messaging Protocol, utilisé dans Flash Media Server. Mais méfiez-vous de tout ce qui brille...

Une nouvelle qui devrait bouleverser l'univers du Net, du moins tout ce qui touche à la vidéo : Adobe vient en effet de rendre publiques dès cette année les caractéristiques de base du Real-Time Messaging Protocol. Né sous le nom de Flash Communication Server MX et développé par Macromedia, ce dernier a été acheté par Adobe parallèlement à Macromedia en décembre 2005. Un système à la base du streaming Flash, celui-là même qui a fait le succès de nombreux sites, dont le plus connu est l'incontournable YouTube. Le protocole RTMP, véritable cœur du serveur, était jusqu'à présent propriétaire, en empêchant ainsi la libre-concurrence sur les plates-formes de streaming et en créant une situation de monopole avec la solution Flash. Les premières réactions ne se sont pas faites attendre, marquées par un certain enthousiasme : dès 2009, n'importe quel développeur pourra créer des programmes avec technologie Flash incorporée, sans payer le moindre centime à Adobe. Les développeurs indépendants pourront ainsi faire leur entrée sur un marché prometteur. Quant aux développeurs de software Open Source, ils pourront créer en toute légalité de nouveaux outils à destination des plates-

Adobe a déclaré qu'elle allait dévoiler cette année les caractéristiques de son protocole RTMP, mais ce n'est certes pas un cadeau, dans la mesure où cela est indispensable à la survie de Flash.

formes les plus diverses. Une simple analyse suffit toutefois à comprendre qu'Adobe n'a pas franchi le pas par gaieté de cœur ; les raisons sont nombreuses, sans oublier la "patte" de Redmond.

:: Silverlight débarque

Ainsi il y a quelques années encore, le statut de monopole d'Adobe sur ce marché était indiscutable.

Les développeurs Adobe peuvent télécharger une version démo gratuite du serveurdestreamingmaisdoiventnéanmoins acheter les outils de développement.

Flash s'était imposé facilement grâce à ses caractéristiques en termes de légèreté et de qualité. Mais en décembre 2006, Microsoft a mis à disposition de sa communauté de développeurs la pré-version d'un système, Silverlight, destiné à concurrencer ce qui était déjà un standard du Web. La première version rendue publique en 2007 n'avait pas inquiété grand monde : lente, elle utilisait une grande quantité de bande non optimisée. Mais après plusieurs versions, la version 2 est enfin sortie en 2008, bouleversant tout sur son passage. Silverlight s'est ainsi révélé tout aussi rapide, stable et flexible que Flash. Parallèlement aux nouveautés techniques, Microsoft a également travaillé sur l'aspect commercial, en signant un accord avec Nokia pour l'intégration de Silverlight dans ses téléphones, en convertissant tous ses sites à Silverlight et en créant et en fournissant gratuitement aux développeurs un kit d'intégration pour leurs programmes (Net). C'est justement cette intégration qui a permis la diffusion instantanée du nouveau format auprès des développeurs, lesquels n'ont rien à acheter pour son utilisation, dans la mesure où cette intégration est disponible gratuitement avec

Microsoft Silverlight est le principal concurrent du streaming d'Adobe et commence à devenir très dangereux : sa diffusion est en nette progression.

les outils de développement qu'ils ont déjà acheté. Et s'ils n'ont rien acheté, ils peuvent tout aussi bien utiliser les versions Express, téléchargeables gratuitement sur le site Microsoft. Une approche bien différente d'Adobe, qui vend non seulement ses plates-formes serveur mais aussi les outils de développement nécessaires.

:: Du Flash en veux-tu en voilà

Officiellement bien sûr, Adobe affirme que sa décision est uniquement liée à son Open Screen Project : le projet en cours depuis plusieurs années, dont l'objectif est de faire de Flash le standard de streaming disponible sur n'importe quelle plate-forme : Ce qui est certainement vrai, aux vues des efforts réalisés par Adobe pour créer des players Flash adaptés à toutes les plates-formes. Mais cela prouve qu'Adobe ne s'attendait certainement pas à la sortie et encore moins au succès de Silverlight. L'ouverture entre Microsoft et sa communauté de développeurs a permis à Silverlight de dépasser immédiatement Flash, grâce à la possibilité de passer à cette

Youtube est sans nul doute le site le plus connu utilisant la technologie de streaming d'Adobe pour Flash.

nouvelle technologie sans débourser un centime : sans changer d'outils, tout en bénéficiant du support Microsoft. La seule carte que pouvait jouer Adobe consistait justement à rendre libres lesdites caractéristiques pour conquérir les programmeurs de l'Open Source. La communauté de développeurs devra faire en sorte de récupérer les outils nécessaires à l'intégration de Flash dans leurs produits. D'un point de vue commercial aucune équipe de manager ne pourra plus choisir de gaieté de cœur Flash comme plate-forme et devra également évaluer attentivement Silverlight : tout ce que redoute Adobe. Une situation qu'elle ne pourra guère modifier tant qu'elle continuera à vendre ses outils de développement.

:: La révélation

Adobe a spécifié qu'aucune information concernant les protections DRM utilisées par sa plate-forme de streaming ne serait dévoilée, toute éventuelle divul-

Silverlightbénéficied'unatoutparrapportà Flash : mêmesansoutilsdedéveloppement, il est possible de les télécharger gratuitement sur le site de Microsoft.

gation rendant inutiles lesdites protections. Cela signifie concrètement que l'application du DRM dans les films Flash ne dépend pas de clés mais du protocole de chiffrage utilisé. Un point qui n'ira certainement pas en faveur d'Adobe, vu les cas précédents tels que le DES, où le reverse engineering a totalement détruit différents systèmes de chiffrement. Les experts en cryptographie voient cette information comme l'indication selon laquelle le système de chiffrement et de protection utilisé par Flash est pour le moins fragile et pourrait être déjà compromis.

Comment les crackers s'y prennent-ils pour vous subtiliser votre compte Windows Live Messenger ?

MSN HACK

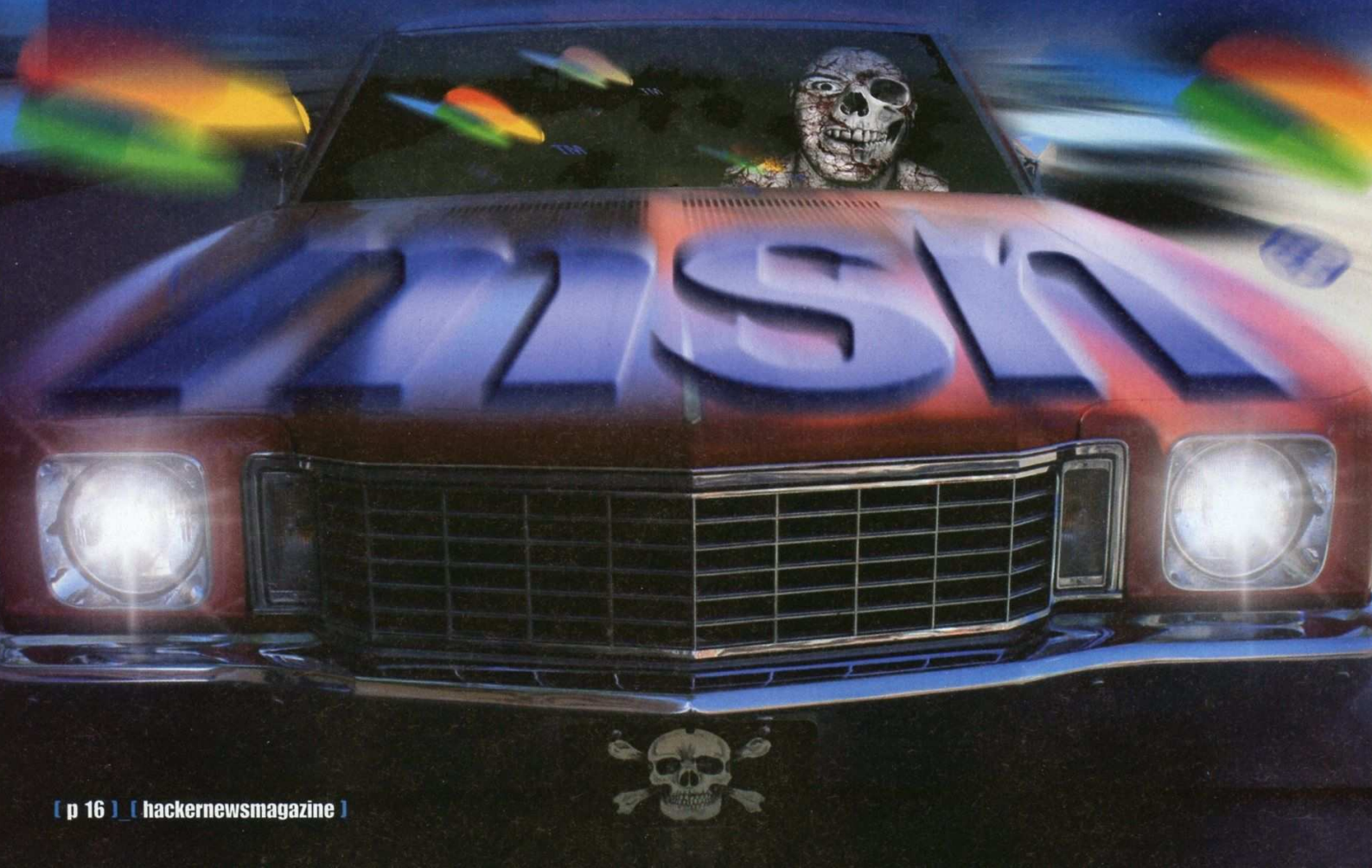
Windows Live Messenger, l'actuelle version de MSN Messenger, bat tous les records de succès à l'instar de la télé, puisqu'il a désormais conquis toutes les maisons. Il permet en effet de se faire de nouveaux amis de façon simple et rapide et de rester en contact avec les anciens. Qui plus est, ses dernières versions vous proposent des outils à la fois utiles et amusants pour accomplir de nombreuses actions. Comme tous les softwares de communication, il doit toutefois être utilisé avec un peu de jugeote.

:: Utilisation normale

En réalité, Windows Live Messenger fonctionne déjà très bien tel quel. Mais c'est dans la nature du hacker de tenter de soulever le capot et de voir ce qui s'y cache, sans doute pour modifier certains éléments, chacun selon ses possibilités. Le minimum que vous puissiez faire ? C'est d'installer Messenger Plus! Live, un add-on qui, à lui seul, permet de modifier de nombreux éléments de cette messagerie. Dans la plupart des cas, il s'agit de changements esthétiques : aspect des fenêtres, possibilité de personnalisation graphique avec les skins, utilisation de couleurs et de styles différents dans le texte et ainsi de suite. Autres fonctions utiles : le regroupement des chats sur une seule fenêtre divisée en onglets, des fonctions avancées pour la gestion de la liste des contacts et la possibilité d'étendre le programme à l'aide de scripts. Ces possibilités sont donc virtuellement infinies, mais restent à la portée de tous.

:: Crackers et MSN

Vu sa large diffusion, on devinera facilement que cette messagerie est un outil utile non seulement pour les utilisateurs normaux, mais aussi pour les "fouineurs".



Vous trouverez une belle collection de script pour Plus! à l'adresse http://www.msgpluslive.it/scripts/browse/

Actuellement largement répandu, MSN Virus est désormais devenu une véritable plaie : un message envoyé par un cracker qui se fait passer pour l'un de vos contacts et vous invite à télécharger une photo ou à visiter un site (la photo, Dieu sait pourquoi, est un exécutable compressé dans un fichier ZIP qui n'est même pas détecté par les antivirus, ce qui devrait déjà vous intriguer...). Dans les deux cas, un programme s'exécute sur votre PC, et envoie au cracker votre login et password MSN, outre le fait de transmettre le même message fictif à tous les contacts présents dans votre liste. Un virus tristement célèbre car, lorsque c'est l'un de vos amis qui est infecté, les messages d'invitation à télécharger le virus maquillé en photo sont tellement agaçants, qu'on est vite tenté de bloquer cet ami jusqu'à ce qu'il résolve le problème. Pour l'aider, vous pouvez l'inviter à effectuer une recherche sur

Dans le cas présent, le virus spécial MSN renvoie la victime sur un site Web, mais la version "locale" existe également en vous faisant télécharger un fichier infecté

Google et à utiliser le programme MSNFix, capable de dénicher et de retirer définitivement le virus. Auparavant, Youtube diffusait des vidéos (retirées pour on ne sait quelle raison) de cracker en pleine action avec ce virus : un programme spécialement écrit crée un exécutable contenant le virus non détectable par les antivirus normaux et le zippe dans un fichier, lequel est envoyé au contact victime. Le plus dur c'est de convaincre la victime - avec un peu d'ingénierie sociale - d'exécuter ce programme, mais une fois cette barrière franchie, le cracker prend le contrôle total de son compte MSN, et peut donc l'utiliser pour transmettre le virus à X autres personnes en attendant qu'elles s'infectent. En laissant le programme ouvert sur son PC, le cracker reçoit automatiquement, dès qu'une victime se connecte, un message contenant le login et password de son compte MSN, et c'est là que le cercle se referme (concrètement, le cracker peut poursuivre indéfiniment son action, jusqu'à ce que des pigeons tombent dans le piège).

:: Webcam hacking

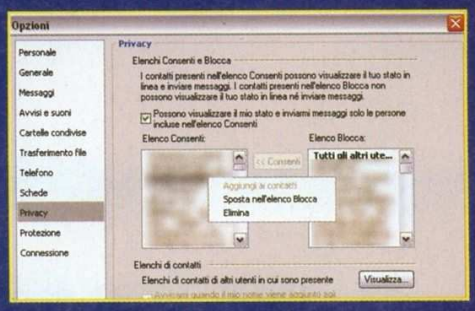
Un procédé semblable permet même de prendre le contrôle de la webcam du contact victime. La clé réside une fois encore dans un fichier qui doit être exécuté par la personne prise pour cible. Dans ce cas, le cracker ne lui vole pas son compte, mais installe un mini-serveur qui envoie l'image filmée par la webcam de la victime à un programme client qui fonctionne sur le PC du cracker. Le plus difficile, si l'on peut s'exprimer ainsi, c'est de dénicher

Cette vidéo sur YouTube montre la procédure et les programmes à utiliser pour voler la vidéo transmise par la webcam du contact victime

l'IP de la victime : des scripts spécifiques peuvent être utilisés à cette fin pour le pack Plus! dont nous avons parlé précédemment. On peut également utiliser la commande netstat /n à partir de l'invite de commandes d'XP et éplucher les IP indiquées jusqu'à trouver la bonne. Il existe enfin un programme qui permet de dénicher l'IP en faisant tout simplement glisser sa fenêtre sur celle de la conversation avec le contact, mais bien sûr, il ne s'agit pas d'un software fiable vu son origine (il est signalé comme dangereux même par les antivirus). Après avoir obtenu l'IP de la victime naïve, on le donne en pâture au programme client et voilà, le tour est joué : une fenêtre à part affiche la vidéo capturée par la webcam. Le seul doute qui persiste, et que les forums du Web n'ont toujours pas éclairci, c'est la façon dont se comporte le témoin d'allumage de la webcam : il semble difficile qu'il puisse rester éteint, mais le cracker s'assurera sans doute que sa victime utilise déjà sa webcam pour "dissimuler" ses activités d'espionnage.

:: Liste des contacts

De nombreux sites promettent de débusquer ceux qui vous ont bloqué ou supprimé de leur liste de contacts. Vous aurez sans doute deviné qu'il s'agit de promesses d'ivrogne : dans certains cas, il s'agit juste un moyen de s'approprier votre adresse ou pire encore, votre compte tout entier. S'il n'existe aucun moyen de dénicher ceux qui vous ont effectivement bloqué, il existe un système (qui n'est toutefois pas infaillible) pour savoir qui vous a supprimé de sa liste : ouvrez la fenêtre des options (Outils/Options) et activez l'onglet Confidentialité. Effectuez un clic droit sur chaque contact présent dans l'encadré



Un système pour vérifier si vous avez été supprimé par l'un de vos contacts

Liste Verte et vérifiez l'état de la commande Supprimer : si elle est en gris et inactivable, alors vous êtes encore dans la liste de ce contact, si en revanche elle est noire et sélectionnable, il vous a sans doute supprimé. Dans Messenger Plus! Live, cet outil est présent sous forme de fonction spécifique (menu Plus!/Nettoyage liste Contacts). Si en revanche vous ne souhaitez pas que l'un de vos amis puisse vous bloquer, vous trouverez une combine pour Messenger Plus! sous forme de script à l'adresse http://software-world.forum-community.net/?t=11008416.

Analysons l'attaque d'un système de routage des paquets d'un LAN pour intercepter ses communications

L'HOMME AU MILIEU NOUS ÉCOUTE

Man in the Middle Attack, un type d'attaque exploité depuis longtemps pour intercepter les communications qui transitent par les câbles réseau, et exploitant une faiblesse intrinsèque du système : les paquets ARP. Ces derniers ne nécessitant aucune authentification, ils peuvent donc être facilement falsifiés. Cette technique permet tout simplement "d'écouter" les communications transitant entre deux ordinateurs (en parvenant à lire les mots de passe non cryptés transmis par certains protocoles) ou provoquer une interruption des services par la plus classique des attaques DoS.

:: Comment ça marche ?

ARP n'est autre que l'acronyme d'Address Resolution Protocol et sert à mapper dans un réseau local l'adresse IP d'un ordinateur avec l'adresse MAC de sa carte réseau. Un fonctionnement qui peut s'avérer utile sur un réseau commuté puisque le système doit savoir à quelle machine adresser un paquet, en interrogeant ainsi le LAN comme suit :"à quelle adresse MAC correspond l'IP x.x.x.x ?" Une fois la réponse reçue, il l'enregistre dans un cache puis continue dès lors à transmettre les paquets avec IP de destination x.x.x.x à l'adresse MAC obtenue suite à la question. C'est un peu comme le fonctionnement du DNS sur Internet : pour accéder à un site, on tape son adresse mnémonique dans le navigateur et le serveur DNS la traduit par l'adresse IP du serveur Web sur lequel il réside. La Figure 1 nous montre un simple exemple de ce fonctionnement :

No.	Time	Source	Destination	Protocol	Info
725	355.536520	192.168.1.10	235.1.1.1	IGMP	V2 Membership Report / Join group 235.1.1.1
726	355.560979	192.168.1.1	224.0.0.1	IGMP	V2 Membership Query, general
727	356.800993	AsustekC_08:7e:92	Broadcast	ARP	Who has 192.168.1.107? Tell 192.168.1.102
728	356.801530	SamsungE_2f:85:48	AsustekC_08:7e:92	ARP	192.168.1.107 is at 00:15:99:2f:85:48
729	356.801536	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request
730	356.801951	192.168.1.107	192.168.1.102	ICMP	Echo (ping) reply
731	357.788681	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request
732	357.789330	192.168.1.107	192.168.1.102	ICMP	Echo (ping) reply
733	358.194734	192.168.1.102	224.0.0.251	IGMP	V2 Membership Report / Join group 224.0.0.251
734	358.788709	192.168.1.102	192.168.1.107	ICMP	Echo (ping) request

***Figure 1** - Un simple ping vers un host du réseau a également généré la demande ARP pour identifier son adresse MAC.*

le host 192.168.1.102 veut pinguer le host 192.168.1.107, une demande ARP est générée pour savoir qui détient l'adresse 192.168.1.107 (ligne 727). Ce dernier répond directement par "moi, c'est 192.168.1.107 et mon adresse MAC est 00:15:99:2F:85:48" (ligne 728) ; après quoi on assiste à la transmission des paquets ICMP de la commande ping, avec les réponses correspondantes (à partir de la ligne 129).

:: Structure d'un paquet ARP

La structure d'un paquet ARP est définie selon le fragment de Code 1, obtenu à partir du fichier if_arp.h dans les sources Linux.

(Code 1)

```
struct  arphdr {
        u_short ar_hrd;         /* Format of hardware address */
        u_short ar_pro;         /* Format of protocol address */
        u_char  ar_hln;         /* Length of hardware address */
        u_char  ar_pln;         /* Length of protocol address */
        u_short ar_op;          /* one of: */
#define ARPOP_REQUEST   1     /* Request to resolve address */
#define ARPOP_REPLY     2     /* Response to previous request */
#define ARPOP_REVREQUEST 3    /* Request protocol address given hardware */
#define ARPOP_REVREPLY  4     /* Response giving protocol address */
#define ARPOP_INVREQUEST 8    /* Request to identify peer */
#define ARPOP_INVREPLY  9     /* Response identifying peer */
#ifdef COMMENT_ONLY
        u_char  ar_sha[];       /* Sender hardware address */
        u_char  ar_spa[];       /* Sender IP address */
        u_char  ar_tha[];       /* Target hardware address */
        u_char  ar_tpa[];       /* Target IP address */
#endif
};
```

:: Exploiter ARP Reply

Précisons tout d'abord qu'ARP n'est pas qu'un simple protocole destiné à associer adresses IP et adresses MAC, mais bien un protocole générique proposant également d'autres possibilités. Ici toutefois, seule nous intéresse l'utilisation de l'IP. En observant la structure, on peut deviner que le champ ar_op est utilisé pour transmettre la commande ARP à proprement dit, par exemple ARPOP_REQUEST ou ARPOP_REPLY, qui identifient le type de paquet (demande ou réponse). Penchons-nous également sur Sender hardware address, Target hardware address et Target IP address, qui stockent, dans l'ordre : adresse MAC du host qui effectue la demande, adresse MAC du host qui répond et adresse IP de ce dernier. Sender hardware et Sender IP indiquent toujours les adresses MAC et IP de celui qui fait la demande, tandis que les adresses du Target changent selon le cas. Lorsqu'on effectue une demande, l'adresse Target hardware est remplie de zéros dans la mesure où elle est inconnue, tandis que Target IP contient l'IP de destination. Dès lors que le host de destination répond, il s'occupe uniquement d'insérer son Adresse MAC au lieu des zéros et de modifier ar_op, de ARPOP_REQUEST à ARPOP_REPLY, en renvoyant le paquet au Sender, et en inversant bien évidemment les adresses Sender qui reprennent à présent les adresses Target, associées au host qui a effectué la demande d'origine. Le Sender initial actualise à présent son cache ARP avec les informations reçues et, jusqu'à l'échéance de ces dernières, les informations du cache ARP ont elles aussi leur propre TTL (Time To Live) comme les paquets TCP ou les données DNS. Il n'effectuera pas d'autres demandes pour connaître l'adresse MAC de Target et poursuivra la communication en prélevant l'adresse de son propre cache. La Figure 2 nous montre en détail la demande ARP, tandis que la Figure 3 nous montre la réponse correspondante.

:: L'attaque

Mais alors que se passe-t-il si quelqu'un s'insère entre le Sender et le Target en falsifiant le contenu des paquets ARP de réponse, et en remplaçant la MAC address Target par la sienne ? Simple à deviner : Sender actualisera son propre cache avec l'adresse erronée et acheminera toutes les futures communications vers l'intrus, lequel pourra les diriger vers la bonne destination pour rendre le passage transparent et, entretemps, analyser le contenu des pa-

```
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: AsustekC_08:7e:92 (00:0e:a6:08:7e:92)
    Sender IP address: 192.168.1.102 (192.168.1.102)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.107 (192.168.1.107)
```

***Figure 2** - Les détails de la demande ARP : notez l'espace consacré au Target MAC paramétré sur zéro, qui sera rempli par le Target avec la réponse.*

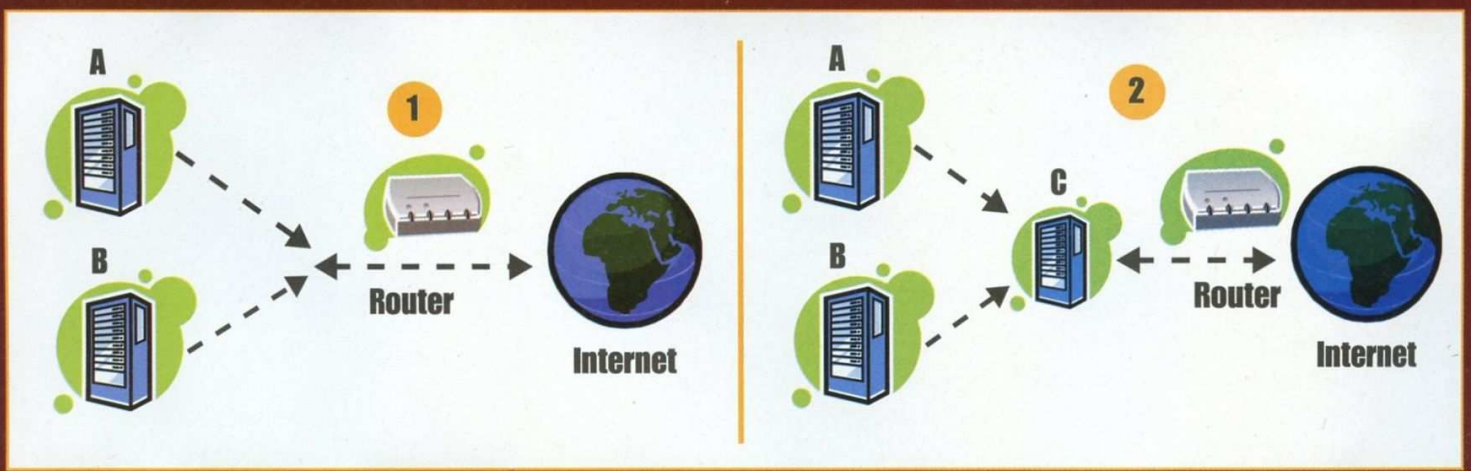
quets. Le classique Man In The Middle. Mais voyons comment ça marche. En utilisant un software pour effectuer un packet injection, l'attaquant veut inciter la victime à créer une entrée dans son propre cache ARP en utilisant une IP inexistante, en injectant de fausses demandes ARP de par l'utilisation du faux Sender IP et de son propre Sender Hardware. En utilisant comme destination FF:FF:FF:FF:FF:FF (c'est-à-dire tout le réseau), on n'obtient aucune réponse, mais en orientant les demandes directement vers le host victime, cela crée la rubrique dans le cache et fournit une réponse adéquate. Dès lors, toutes les communications réseau de la victime seront également reçues par l'ordinateur de l'attaquant, lequel se contente de les capturer pour pouvoir les enregistrer et les réacheminer en réseau pour agir de façon transparente.

```
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: SamsungE_2f:85:48 (00:15:99:2f:85:48)
    Sender IP address: 192.168.1.107 (192.168.1.107)
    Target MAC address: AsustekC_08:7e:92 (00:0e:a6:08:7e:92)
    Target IP address: 192.168.1.102 (192.168.1.102)
```

***Figure 3** - Même détail concernant la réponse du Target : les adresses Target et Sender sont inversées et la commande ar_op transformée en Reply.*

:: Comment se défendre ?

Si tout cela est possible, comme nous l'avons déjà dit, c'est parce que le protocole ARP n'exige aucune authentification. Les ordinateurs "se fient" donc à ce qu'ils reçoivent. Pour se défendre contre ce type d'attaque, on peut, par exemple, adopter IPv6, IPsec ou encore adopter des tableaux ARP statiques. Si vous avez la possibilité de surveiller vos communications réseau, en utilisant un paquet comme arpwatch, vous pourrez alors déceler immédiatement tout comportement anormal et prendre les contre-mesures qui s'imposent. En alternative, vous pouvez également adopter SARP, ou Secure ARP, une extension de ce protocole, à même d'authentifier le Sender, ou d'implémenter le port security des switch réseau, qui force la correspondance de chaque port du dispositif avec une seule adresse MAC. Mais la meilleure solution consiste encore à mettre en place un réseau 802.1x avec serveur RADIUS, qui force l'authentification distante. Dans tous les cas, mieux vaut toujours rester sur ses gardes : sniffer de temps à autres le trafic de son propre réseau n'est jamais inutile.

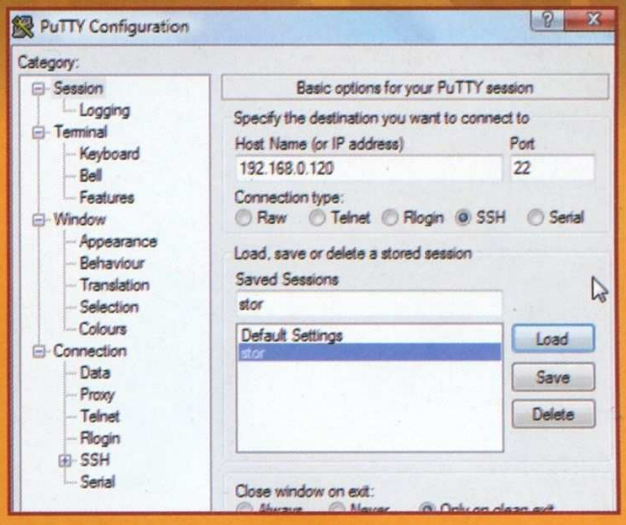


Sur le schéma 1, le flux d'une communication normale ; sur le schéma 2, en revanche, l'attaque classique de type "Man in the Middle" : l'ordinateur C, celui du Hacker, intercepte la communication entre les machines A et B en feignant d'être un PC agréé du réseau.

Transformer un réseau de stockage en machine à télécharger des torrents

Hacking & Download

La distribution de fichiers par le biais du système Torrent permet d'optimiser les partages de fichiers entre les différentes sources. Malheureusement, la plupart des fichiers torrent restent longs à télécharger et nous contraignent à laisser l'ordinateur allumé pendant de longues heures. Et lorsqu'on possède un ordinateur portable, le téléchargement d'un ou plusieurs fichiers torrents empêche toute déconnexion et, donc, toute possibilité de l'emporter avec soi, sous peine de devoir récupérer les téléchargements, avec la perte de temps qui en découle. En outre, à bien y réfléchir, la puissance de nos ordinateurs est totalement gaspillée pour les téléchargements, alors qu'un processeur rapide est en réalité totalement inutile. Un processeur quelconque suffit amplement, avec une connexion réseau classique. L'important étant l'espace disque, nécessaire pour pouvoir télécharger tout ce que l'on souhaite. Des caractéristiques auxquelles répondent parfaitement des disques externes comme certains des MyBook produits par Western Digital. Les WD MyBook World Edition I et II, tout comme le WD ShareSpace, sont en effet composés d'un ou plusieurs disques couplés à une carte mère sur laquelle est installée une version embed-



Putty est un utilitaire gratuit à télécharger sur www.chiark.greenend.org.uk/~sgtatham/putty. Il est le meilleur outil pour accéder aux dispositifs avec softwares embedded.

ded de Linux, avec une carte réseau utilisée pour les relier au réseau domestique ou à celui de l'entreprise. Sur le papier, tout le nécessaire est là pour transformer l'une de ces unités de stockage en système de téléchargement autonome, en libérant ainsi notre ordinateur de cette fonction. Naturellement, la modification de ces dispositifs met fin à la garantie du fabricant mais vu leur potentiel, dans la plupart des cas, le jeu en vaut largement la chandelle.

:: Ouverture des verrous

La première chose à faire, c'est de trouver la façon d'accéder directement au système d'exploitation du disque, en by-passant l'interface Web de gestion standard. Et pour cela, voici un petit truc : pour mettre à jour son firmware, ce type de disques effectue une connexion Web vers un site spécifique et il suffit de mélanger un peu les cartes pour faire effectuer au dispositif un script différent. Entrez dans l'interface Web de gestion du disque en tapant votre nom et votre mot de passe. Accédez ensuite à la mise à jour du firmware de l'unité et modifiez la partie finale de l'adresse par ?fwserver=mybook1.110mb.com/firmware.php. Vous devriez obtenir un message similaire à celui de la Figure 1 : Tapez sur Entrée puis cliquez sur Download and Install pour mettre à jour le firmware. En réalité, le disque ne fera que débloquer un protocole d'accès appelé SSH, par le biais duquel vous accéderez à ses fonctions de base. Quelques minutes plus tard, le tour est joué et le dispositif débloqué. Vous avez à présent besoin d'un programme de gestion du protocole SSH pour accéder au disque. Putty compte parmi l'un des meilleurs du marché, gratuit qui plus est. Téléchargez-le sur http://www.chiark.greenend.org.uk/~sgtatham/putty/ et installez-le. Une fois lancé, et après avoir tapé l'adresse de votre disque réseau, en laissant tels quels les autres paramètres, vous vous retrouverez face à la console Linux. Tapez à présent le nom d'accès que vous utilisez aussi pour l'interface Web standard et le mot de passe correspondant pour ouvrir une session authentifiée. A présent, il suffit de taper la commande su-, sans mot de passe, pour devenir administrateur root du système. En paramétrant un mot de passe, comme pour toute autre version de Linux, vous pourrez accéder au système directement par le biais du compte root.

```
login as: root
root@192.168.0.120's password:
[root@KhamulStorage ~]# /opt/bin/ipkg update
Downloading http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable
/Packages.gz
Inflating http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable/P
ackages.gz
Updated list of available packages in /opt/lib/ipkg/lists/optware
Successfully terminated.
[root@KhamulStorage ~]# /opt/bin/ipkg install transmission
Installing transmission (1.42-1) to /opt/...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable
/transmission_1.42-1_arm.ipk
Installing libcurl (7.19.2-1) to /opt/...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable
/libcurl_7.19.2-1_arm.ipk
```

Après avoir obtenu l'accès au disque par le biais de Putty, l'installation des utilitaires s'effectue comme pour n'importe quelle version standard de Linux.

(Figure 1)
http://192.168.10.120/auth/firmware_upgrade.pl?fwserver=mybook1.110mb.com/firmware.php

:: Quelques utilitaires

L'étape suivante consiste à installer quelques suites de programmes utiles à votre survie. La version de Linux à votre disposition est malheureusement réduite à son strict minimum. Commencez par installer le gestionnaire de paquets OptWare, avec lequel vous installerez tout le reste. Vous devez pour cela le récupérer comme si vous étiez dans une installation Linux classique, par le biais des feeds. Il suffit d'utiliser la suite de commandes indiquées en bas de la Figure 2. OptWare est maintenant installé, mais de par les caractéristiques de la version de Linux à votre disposition, vous allez devoir ajouter un paramètre au fichier de configuration de ld. Vous allez ainsi devoir taper deux dernières commandes : echo "/opt/lib" >>/etc/ld.so.conf ldconfig

Après cette installation, vous allez enfin pouvoir installer un bon éditeur de textes, comme Nano, parfaitement adapté à votre disque externe. Pour cela, utilisez OptWare :
/opt/bin/ipkg install nano

Avec Nano, vous allez pouvoir ouvrir **/etc/inittab** et ajouter la ligne suivante, pour rendre le SSH disponible même en cas de redémarrage du disque : **sysinit:/usr/sbin/sshd**

Le système Linux présent sur le disque externe est maintenant prêt à être façonné à votre gré, et vous allez pouvoir l'utiliser comme une distribution Linux normale.

(Figure 2)

```
feed=http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable
ipk_name=$(wget -qO- $feed/Packages | awk '/^Filename: ipkg-opt/ {print $2}')
wget $feed/$ipk_name
tar -xOvzf $ipk_name ./data.tar.gz | tar -C / -xzvf -
sed -i -e 's|stable|unstable|' /opt/etc/ipkg.conf
```

:: Feu vert aux download

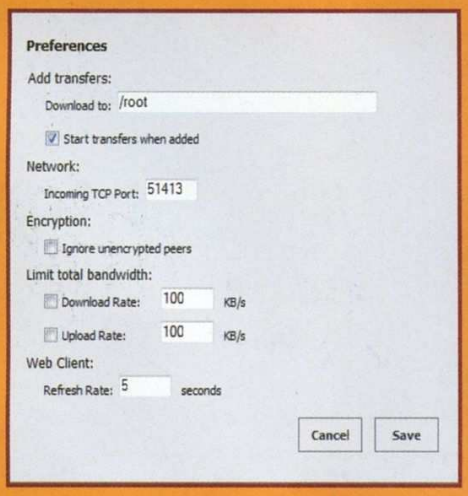
Pour créer un système de téléchargement de fichiers torrents, vous devez installer Transmission, un client on ne peut plus célèbre fonctionnant en environnement Linux, mais disponible pour différentes plates-formes.

[Figure 3]

```
/opt/bin/ipkg update
/opt/bin/ipkg install transmission
ldconfig
/opt/bin/ipkg install libiconv
ldconfig
```

Toujours en utilisant OptWare, il vous suffira de taper les commandes décrites à la Figure 3 : une fois l'installation terminée, vous pouvez lancer Transmission en utilisant la commande suivante :/opt/bin/transmission-daemon

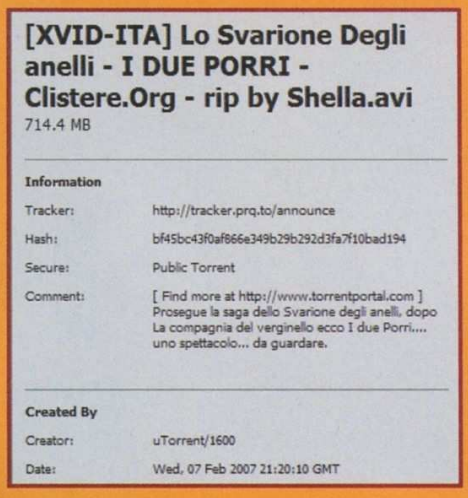
Dans la plupart des cas, cela ne vous suffira toutefois pas à vous autoriser l'accès au site de téléchargement : comme paramètre standard, Transmission n'accepte les connexions que si elles proviennent de la machine même, avec IP 127.0.0.1. Il serait peu logique d'utiliser le système SSH pour indiquer vos téléchargements alors que Transmission met à votre disposition une interface Web très pratique. Pour toute modification, vous allez devoir arrêter le processus de Transmission avec la commande suivante : **# killall transmission-daemon.**



Le site Web activé sur le port 9091 permet de contrôler les téléchargements et de paramétrer vos préférences en termes de fonctionnement

```
    "blocklist-enabled": 0,
    "download-dir": "\/root",
    "download-limit": 100,
    "download-limit-enabled": 0,
    "encryption": 0,
    "max-peers-global": 200,
    "peer-port": 51413,
    "pex-enabled": 1,
    "port-forwarding-enabled": 0,
    "rpc-authentication-required": 0,
    "rpc-password": "",
    "rpc-port": 9091,
    "rpc-username": "",
    "rpc-access-control-list": "127.0.0.1,192.168.0.*",
    "rpc-whitelist": "127.0.0.1,192.168.0.*",
    "upload-limit": 100,
    "upload-limit-enabled": 0
}
```

Utilisez nano, un éditeur de textes basique, pour modifier les paramètres par défaut de Transmission et autoriser l'accès au système à partir de n'importe quelle IP de votre réseau LAN



Il vous permet de consulter différentes informations sur les fichiers en cours de téléchargement : taille, temps de téléchargement, hash du fichier, etc.

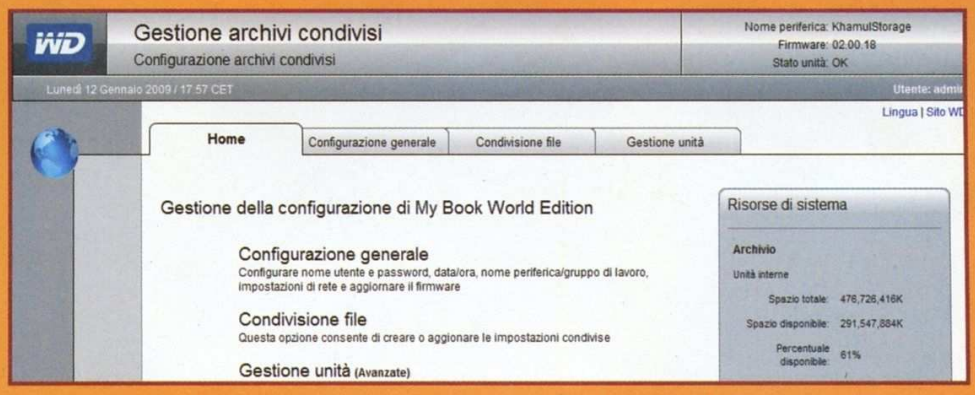
Puis, à l'aide d'un éditeur de textes, vous allez devoir modifier le fichier **/root/.config/transmission-daemon/settings.json** en modifiant les lignes suivantes. Certes, si vous disposez d'un réseau avec une autre adresse que celle-ci 192.168.1, vous allez devoir adapter les données entrées à votre cas personnel,

[Figure 4]

```
"rpc-access-control-list": "127.0.0.*,192.168.1.*",
"rpc-whitelist": "127.0.0.1,192.168.1.*",
```

voir **Figure 4**. Enregistrez le fichier, redémarrez Transmission et connectez-vous avec votre navigateur à l'adresse correspondant à votre disque, sur le port 9091 : **http://192.168.10.120:9091/**

Vous trouverez une interface Web prête à accueillir vos demandes de téléchargement.



L'installation de programmes supplémentaires annule la garantie mais n'altère en aucun cas l'interface standard de gestion du disque.

Découvrez le fonctionnement de l'une des attaques les plus simples et dangereuses

DNS EMPOISONNÉS

Ce type d'attaque n'a rien de nouveau, puisqu'il existe depuis plus de 10 ans : le danger vient des serveurs DNS qui, pour communiquer entre eux, utilisent des références (Query ID) assez faciles à prévoir. Cette attaque est plus facile qu'on ne l'imagine. Le programme BIND est facilement accessible depuis Internet. Il suffit ainsi d'étudier le programme et d'un peu de pratique pour se rendre vite compte de la vulnérabilité du centre névralgique des serveurs DNS.

:: Mode de fonctionnement

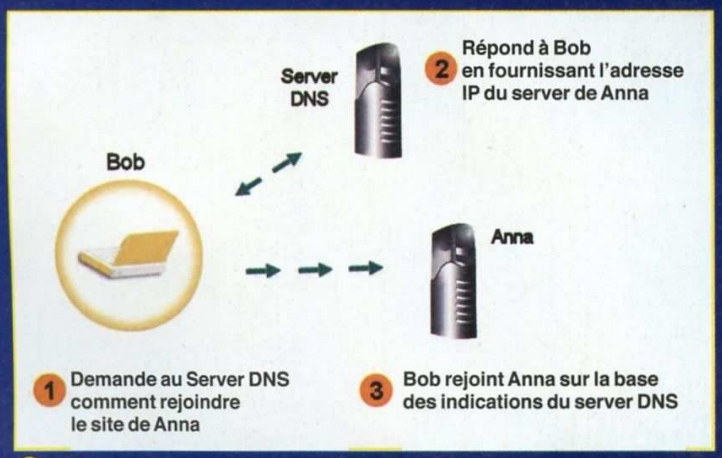
Tout d'abord, à quoi les serveurs DNS jouent-ils pendant toute la journée ? Ils transforment des noms comme www.google.fr en adresse IP (ex. 123.12.134.123) compréhensible par les machines et contenant toutes les informations pour accéder au serveur souhaité. Mais si le lien entre un site et sa véritable adresse IP est modifié, la communication est alors détournée vers une autre adresse IP. Ce qui a tout l'air d'une mauvaise plaisanterie. Plaisanterie qui peut toutefois vite tourner au vinaigre quand on pense par exemple aux services bancaires online : vous vous connectez, donnez votre nom d'utilisateur et votre mot de passe au site factice qui se fait passer pour celui de votre banque pendant que quelqu'un accède à ladite banque en utilisant vos données et votre argent.

:: DNS canonique

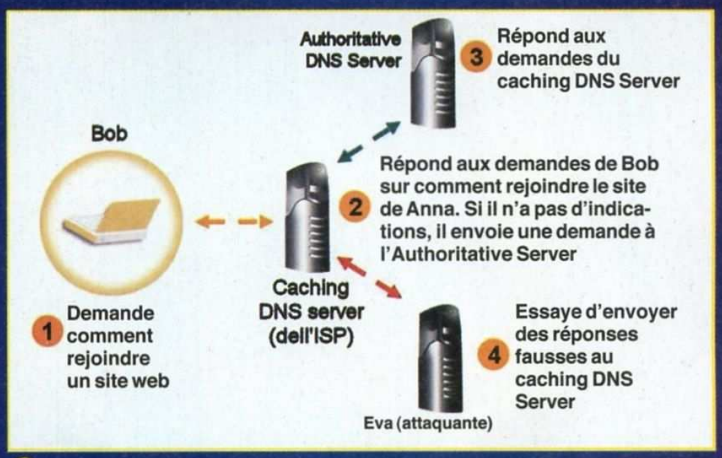
Lors d'une communication sur le Web, avant que les informations n'apparaissent sur votre navigateur, votre requête passe par différentes étapes dont vous n'avez généralement aucune notification. Si vous recherchez par exemple www.google.fr, votre navigateur transmet votre demande, laquelle est envoyée jusqu'au premier DNS disponible représenté dans le Schéma 1. L'information sur la durée de vie du site de votre dernière demande DNS est expressément fournie par le Serveur B (en admettant que B ait trouvé cette information dans sa liste). Son nom ? Le TTL (Time to Live). Arrivée à échéance, la demande doit être à nouveau vérifiée.

:: Le maillon faible

La Query ID, ou QID, sert à maintenir classées et séparées les différentes demandes adressées au serveur. C'est un peu comme le ticket que vous prenez au supermarché pour faire la queue. Chaque client a son numéro et le commerçant sert les clients un à un en suivant l'ordre des numéros de ticket. Par convention, les 16 premiers bits des



Dans une demande DNS normale, le resolver (Bob) souhaite savoir comment accéder au serveur d'Anna et en fait la demande au serveur DNS, qui répond par l'adresse IP correspondant au bon serveur



Dans une attaque DSN cache poisoning, Eva envoie de fausses réponses au serveur jusqu'à ce que la QID soit correcte. Le cache du serveur ISP est modifié jusqu'à l'échéance du TTL avec l'IP malveillante

paquets TCP sont utilisés pour entrer cet identifiant univoque. Ce système présente une vulnérabilité certaine. Supposons que Bob soit le resolver et Anna un serveur DNS. Eva est quant à elle cachée dans l'ombre. Bob se connecte à Anna et lui demande l'adresse www.victime.com. Anna trouve dans sa liste que 1.2.3.4 = www.victime.com, mais Eva souhaite que la réponse soit 6.6.6.0. Dans la mesure où Eva ne peut pas voir la QID des paquets de Bob, sa QID ne coïncidera pas avec celle de Bob. Telle est la défense dont Bob dispose pour sa navigation, mais habituellement l'attaque QID, a commencé bien avant et le serveur continue de recevoir les demandes d'Eva. Entre-temps BIND incrémente simplement la QID pour chaque réponse, à l'instar de l'étiquetage dans le commerce. Le serveur DNS crée donc ses QID, par exemple 4001 puis 4002 : vous n'aurez donc aucun mal à deviner que la prochaine QID sera 4003 ! Eva tente donc d'envoyer une réponse avec la QID 4003 ; si elle y parvient, alors Eva a gagné !

:: Empoisonner le cache

Bien sûr, si la génération des QID était totalement aléatoire et un peu plus sûre, le problème n'existerait pas. Mais revenons-en à la connexion. Anna voit que Bob lui a envoyé des paquets de données et connaît également la bonne QID, tandis qu'Eva doit essayer de la deviner ou de la découvrir. Le premier des deux qui parviendra à envoyer le paquet avec la bonne QID l'emportera. Les chances de réussite d'Eva sont toutefois minces. Qui plus est, si elle perd cette partie, elle ne pourra plus retenter sa chance pendant un long moment, les informations sur le cache ayant été validées jusqu'à la TTL. Mais elle pourrait retenter son coup avec un autre schéma et multiplier ainsi ses chances de succès. Les noms www.victime.com, clients.victime.com ou ma.victime.com sont transmis à la même machine, les enregistrements dans le cache du serveur DNS sont donc identiques. Ce qui engendre toutefois une erreur de logique : en créant une série de fausses query pour 1001.victime.com, 1002.victime.com et ainsi de suite, Eva pourrait finir par deviner la QID arrivée au nom 1099.victime.com, et donc modifier le fichier cache du serveur DNS. Le serveur enregistrera les informations supplémentaires pour le nom de domaine 1099.victime.com dans une section du fichier cache spécifique, dénommée additional section. Une fois la mise à jour terminée, toutes les futures demandes pour victime.com effectuées sur ce serveur, par Bob mais aussi par tous les utilisateurs qui souhaiteraient le visiter, seront détournées vers l'IP 6.6.6.0 comme le souhaitait Eva.

(Schéma 1)

1) tapez www.google.fr dans votre navigateur ;
2) votre navigateur demande au système de gestion réseau d'être mis en contact avec le site www.google.fr ;
3) le système cherche dans le fichier hosts s'il trouve une correspondance mais ne la trouve pas ;
4) il contacte le serveur du fournisseur d'accès ;
5) l'ISP contacte le premier serveur DNS et envoie la demande ;
6) si le serveur DNS en question, appelons-le A, ne contient pas l'information relative à l'endroit où se trouve google.fr, il initialise alors une demande à son serveur DNS le plus proche ;
7) le serveur qui reçoit la demande, appelons-le B, se charge avant tout de créer une Query ID, puis se met à rechercher le nom. S'il ne le trouve pas, il interroge alors un autre serveur et ainsi de suite ;
8) si la correspondance est trouvée, votre navigateur, une fois que le Serveur A aura pris note dans son cache, sera mis en contact avec le site et vous pourrez enfin rechercher ce qui vous intéresse.

:: Conclusions

Des personnes malveillantes se sont rendues célèbres de par leurs attaques par empoisonnement de cache DNS. Aujourd'hui, les défenses ont été améliorées et les serveurs DNS patchés pour éviter ce type d'attaque. BIND a été amélioré dans ses dernières versions. Mais la mise à jour effective des serveurs avance au ralenti et il faudra plusieurs années avant que l'on puisse éviter totalement des attaques DNS cache poisoning.

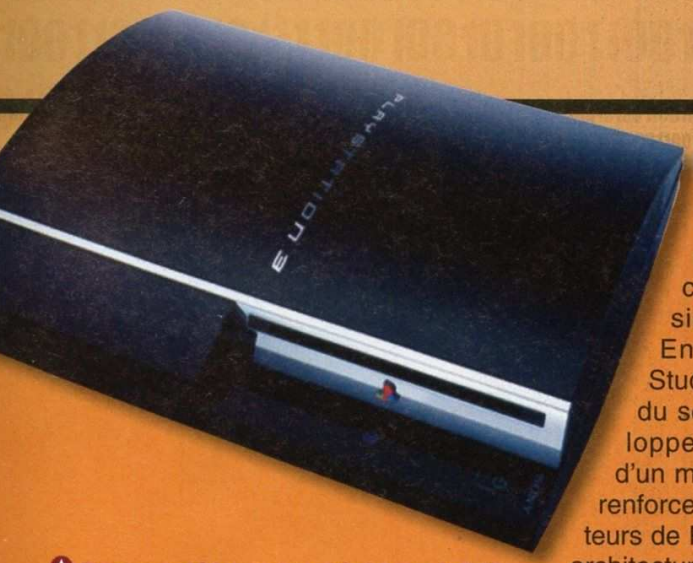
"HOME": BUG DANGEREUX

Sortie du social network 3D pour la console Sony, où quelques ombres subsistent, surtout côté sécurité

Après plusieurs mois de développement, mêlant bruits de couloir et attente interminable, sans oublier plusieurs avant-premières, voici enfin le Playstation Home. Il s'agit d'un social network totalement dédié à Second Life, véritable monde virtuel où les joueurs se rencontrent, lient amitié, organisent des parties et, dans les prochains projets de Sony, feront même leurs achats online. Pas mal de projets en cours, notamment si l'on considère que toutes ces formes d'interaction reposent sur une structure réseau relativement complexe, enrichie d'un graphisme 3D qui, sur le papier du moins, exploite tout le potentiel de l'élégante architecture hardware de la PS3. Oui, "sur le papier", car en réalité, de nombreuses critiques se sont élevées sur ce service. De nombreuses mises à jour ont permis de régler plusieurs défauts, même si beaucoup reste encore à faire.

:: Quelques erreurs de trop

Et pour être tout à fait franc, à l'heure où nous écrivons, l'un des principaux problèmes et non des moindres court toujours parmi les lignes de code de Home :



Par rapport à la version précédente, la PS3 intègre un support Internet efficace. Il faut disposer des bons programmes

tout le monde sait aujourd'hui que le développement de Home a pris à la légère certains aspects liés à double titre à la sécurité informatique. Et il y a de quoi s'inquiéter, car ce sont les données personnelles de millions d'utilisateurs qui sont en jeu. Mais procédons par ordre. Les chroniques racontent que le projet Home est en réalité issu du jeu vidéo "The Getaway Online", version multijoueur d'un titre qui, malgré des coûts de développement dignes d'une production hollywoodienne, fut un demi-fiasco en termes de ventes. Au point, justement, que le projet "Online", dont le travail commença avant la commercialisation du titre d'origine, fut ensuite stoppé. Quelques temps plus tard, Phil Harrison, fraîchement débarqué chez Sony en tant que président de Sony Computer Entertainment Worldwide Studio (concrètement le chef" du service recherche & développement), sponsorisa l'idée d'un monde virtuel grâce auquel renforcer la communauté d'utilisateurs de PS3. Et vu qu'au fond, une architecture technologique était déjà prête, pourquoi ne pas l'utiliser ? Aussitôt dit, aussitôt fait, des cendres de "The Getaway Online", naquit Home. Dommage que les efforts liés à la modernisation du projet n'aient concerné que la partie "visible" de l'iceberg, à savoir le son et le graphisme. On a en effet l'impression que le cœur même du projet, c'est-à-dire les fonctions online, ont été empruntées un peu trop lourdement au titre destiné à l'origine à la Playstation 2, et conçu à une période (2003) où les technologies Internet n'étaient pas aussi abouties qu'aujourd'hui.

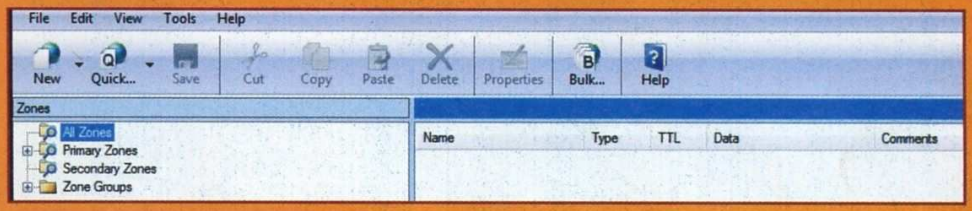
Une bonne partie de la structure de "Home" est directement issue de "The Getaway Online"

:: Graphisme et sécurité

Retour en 2009. Après une phase de contrôle interne, Home est officiellement lancé. Mais quelques jours à peine après sa sortie, les pépins commencent, compte tenu également des nombreuses mises à jour. Citons par exemple les problèmes de graphisme, révélés par les vidéos diffusées sur http://www.youtube.com/watch?v=0DWIcSuJ8TE et sur http://www.youtube.com/watch?v=_UPMnFFolt4&NR=1. Ou encore ceux en matière de sécurité. Il est en effet apparu que la connexion entre chaque console et les serveurs de Sony qui gèrent Home, ne faisait l'objet d'aucune protection. Non, ce n'est malheureusement pas une blague : aucun type de cryptage n'est prêt à codifier les données reçues et transmises de et vers les serveurs, ce qui permet à n'importe quelle personne malintentionnée d'appliquer les techniques de sniffing les plus élémentaires. Sony a-t-il résolu immédiatement le problème ? Pensez-vous ! Tout ce qu'il s'est contenté de faire, c'est de bâillonner tous les sites qui en parlent, sans agir et en faisant peser une vulnérabilité qui fait craindre le pire aux utilisateurs malchanceux !

:: Notions de base

Les modifications apportées sont exploitables à partir de la console d'origine. On arrive ainsi au cas extrême d'un utilisateur du site PS3Hax.net, qui est parvenu à changer certains des posters qui ornaient le monde virtuel de Sony. La technique est élémentaire : après avoir installé Apache HTTP Server, téléchargeable sur (http://rapidshare.com/files/173698264/apache_2.2.10-win32-x86-openssl-0.9.8i.msi), et Simple DNS Plus (la version "trial" est largement suffisante), téléchargeable sur http://rapidshare.com/files/173697154/sdnsplus-setup.exe, allez dans le sous-dossier /Program files/Apache Software Foundation/Apache 2.2/htdocs. Procédez à l'extraction des fichiers de l'archive téléchargeable sur http://bluehost.to/dl=7qjYfKcaL. Après cela, lancez Simple DNS Plus. Cliquez sur Records puis sur Quick. Dans Zone Name, tapez sceehome.playstation.net, tandis que dans Web server IP, vous entrerez votre adresse IP. A présent, à partir du menu de la PS3, allez à la section Network, paramétrez le serveur DNS sur «manuel» et insérez ici aussi votre adresse IP. Allez ensuite dans htdocs, sur c.home\prod\live\Screens. Et là, surprise : vous y trouverez le fichier CinemaChannels.xml. En l'ouvrant, vous allez trouver le nom des fichiers vidéo qui sont affichés dans le cinéma (au format mov, mais les mp4 sont eux aussi supportés). Il suffit de modifier le nom des fichiers et le tour est joué. Tout ce qu'il vous reste à faire, c'est redémarrer Home pour rendre les modifications effectives.



Simple DNS Plus met K.O. le système de sécurité de Home

PICODRIVE

La bonne vieille SEGA megadrive renaît sur votre mobile !

Que celui qui n'a jamais joué avec une console lève la main ! Tandis qu'on assistait autrefois à une guerre ouverte entre PC et Amiga et alors que le PC était sur le point de remporter la victoire, poussé par des légions de clones, avec ses premières cartes audio et vidéo, le marché commença a être envahi de nouvelles consoles exclusivement consacrées au jeu, avec des performances nettement supérieures à celles auxquelles nous étions habitués, bien qu'à des années lumière d'une Playstation 3, par exemple. Parmi celles-ci, on retiendra le succès sans précédent de la SEGA Megadrive, dont bon nombre se souviendront de la mascotte, Sonic le hérisson. Avec les consoles, débarquèrent également de nombreux jeux qui remplirent les journées des ados et autres fans ou nostalgiques de leur jeunesse, et qui aiment toujours et préfèrent même les anciens titres, et ce malgré la profusion d'effets spéciaux des consoles actuelles. Pour satisfaire ces désirs et sans doute aussi par amour du défi, différents émulateurs ont vu le jour pour nous permettre de continuer à jouer avec ces vieux titres, même sur d'autres plates-formes que les originales, comme les PC et même d'autres consoles. Aujourd'hui, il est même possible de transformer en émulateur son téléphone portable, grâce à symbian et à la grande puissance de calcul des processeurs. Et PicoDrive est justement le porting de l'émulateur de SEGA Megadrive pour Symbian !

:: L'émulateur et les ROMS

Ce software est gratuit, méfiez-vous donc des sites proposant un téléchargement payant ou nécessitant une inscription. Voici deux liens où trouver l'émulateur pour différentes versions de symbian : l'installation est on ne peut plus simple : il suffit de décompresser l'archive et d'installer le tout en utilisant PC Nokia Suite. Le software "émule" le hardware des consoles, en permettant de choisir jusqu'au type de puce audio préféré, mais n'espérez pas y trouver le moindre jeu, ou ROM. La question des ROMS reste ouverte dès lors qu'il s'agit de code propriétaire toujours protégé par le copyright, avec toutefois des produits désormais introuvables dans le commerce (si l'on exclut les ventes sur ebay). N'oubliez donc pas que, du point de vue juridique, les

pour S60 2nd version :
http://phonesymbian.com/wpcontent/uploads/2007/12/picodrives602nd060.zip
pour S60 3rd version :
http://phonesymbian.com/wpcontent/uploads/2007/01/picodrive0_50_3rd.zip

ROMS devraient uniquement être utilisées par le propriétaire légitime de la version originale du jeu (voire avec l'autorisation du fabricant) ; il existe en fait tellement de sites proposant ce type de téléchargement (avec la possibilité de conserver de nombreux jeux introuvables ailleurs) que le phénomène est dans la pratique toléré, du moins concernant les ROMS de consoles introuvables dans le commerce (où leur utilisation ne porte donc pas atteinte à un business aujourd'hui disparu). Voici un site parmi tant d'autres qui vaut le détour www.romnation.net. Nous vous conseillons de télécharger les ROMS avec un point d'exclamation, indiquant un dumping à la fois correct et fidèle de la mémoire originale.

:: Installation et utilisation

Vous pouvez choisir d'installer l'émulateur dans la mémoire du téléphone ou dans la mémoire externe. Idem pour les ROMS que nous vous conseillons vivement d'installer dans la mémoire externe. Aucun paramètre particulier n'est nécessaire, vous pouvez donc créer un dossier ROM dans lequel copier toutes celles avec lesquelles vous pourrez jouer. Le programme est installé dans le menu principal. Une fois lancé, vous verrez s'afficher un menu très simple et intuitif.

Le menu de Picodrive

:: PicoDrive en action

L'émulateur supporte les cheats (Game Genie) et patch ROM ; un soft-reset a été prévu pour relancer la ROM sans avoir à la recharger. Vous pouvez choisir le format de l'écran (portrait, full resolution, et même avec un défilement horizontal pendant le jeu) ainsi que le type de rendu (à modifier uniquement en cas de problème graphique). Il est possible d'activer un contrôle plus précis sur la synchronie du jeu et sur les sprites, qui influencent la vitesse et la fluidité de jeu. La ROM peut être figée sur une macro-région (comme les DVD), mais un sélecteur permet de choisir celle qui vous convient. La rubrique Load ROM ouvre votre navigateur pour charger la ROM, tandis que Load/Save permet de geler le jeu au format compressé. Pendant le jeu, si vous avez l'impression de perdre toute synchronisation avec le son, il vous suffit d'appuyer deux fois sur "C" pour régler le problème. En appuyant une seule fois pendant le jeu, vous reviendrez au menu de l'émulateur. Le téléphone peut se bloquer totalement si un coup de fil arrive, un message "Batterie déchargée" apparaît ou encore lorsqu'on passe à une autre application. Avant d'effectuer l'une de ces opérations, mieux vaut donc se rendre dans le menu principal. Si la vitesse de jeu est trop lente ou si l'émulateur bugue, il convient d'activer les puces audio, "accurate sprites" et "accurate timing" et de désactiver "alt. render". Et si les problèmes persistent, activez "alt. render". Si ça ne marche pas non plus, alors mieux vaut faire un rapport sur ce jeu pour informer les autres utilisateurs de ses problèmes de fonctionnement ! En effet, tous les jeux ne sont pas forcément totalement compatibles (par exemple "Virtua Racing" ne fonctionne pas en l'absence d'émulation de Sega Virtua Processor).

Le file browser pour le choix de la ROM

Le menu de configuration vidéo

L'attaque par Déni de Service basée sur les sms, rend le géant finlandais complètement fou

Curse of silence : la malédiction des Nokia

Si l'on vous dit que votre mobile tournant sous Symbian peut être rendu totalement insensible aux sms sans que vous vous en aperceviez, vous y croyez ? Eh oui, c'est possible : Tobias Engel a publié un article détaillé sur une faille de Symbian. Il s'agit d'une attaque à distance par Déni de Service, transmise par sms/mms et surnommée "Curse of Silence" de par l'effet qu'elle provoque : le téléphone victime n'avertit pas l'utilisateur quant à l'arrivée du message malveillant. Par la suite, il ne pourra plus recevoir d'autres messages jusqu'à ce qu'un hard-reset soit effectué (en réinitialisant les paramètres d'usine et en supprimant par la même occasion toutes les données du répertoire, applications, téléchargements effectués, liens du navigateur...).

Les versions de Symbian dotées de la faille sont toutes celles installées sur les Nokia série 2.6, 2.8, 3.0 et 3.1. Autrement dit, presque tous les Nokia tournant sous Symbian sont concernés.

Les versions S60 2.8 et 3.1 encourent un risque moyen, car pendant l'attaque, le mobile ne pourra plus recevoir d'autres sms ou mms. Par la suite, il ne pourra en recevoir que certains jusqu'au reset hardware ; les versions 2.6 et 3.0 encourent en revanche un risque élevé, car suite à l'attaque, le mobile ne pourra plus du tout recevoir de sms ou mms jusqu'à sa réinitialisation !

:: La faille

Le standard 3GPP TS 23.040 spécifie la méthode à utiliser pour envoyer des e-mails via sms. Pour ce format, le sms doit notamment commencer par le champ from- ou to-email-address suivi d'un espace puis du message. Dans ce cas, l'identifiant du message sms doit être paramétré en tant qu'"Internet Electronic Mail". Ce standard ne spécifie toutefois pas la façon dont ce message doit apparaître lorsqu'il est reçu par le téléphone du destinataire, un choix qui est laissé au constructeur (Nokia dans le cas présent).

Avant la version 2.6 du S60, les messages étaient affichés exactement tels qu'ils étaient envoyés. Depuis la version 2.6, lorsque la partie du message censée contenir l'adresse de l'expéditeur a tout l'air d'une adresse e-mail (l'@ apparaît par exemple quelque part), ce champ est affiché comme e-mail expéditeur au lieu de TP-Originating-Address.

Si ce champ est composé de plus de 32 caractères, les quatre versions incriminées de Symbian échouent alors dans l'affichage du message ou dans la notification de son arrivée sur l'interface, mais envoient au centre de messagerie la confirmation de sa réception. Si un e-mail est donc envoyé par le biais d'un sms avec le formatage suivant :
où l'adresse e-mail contient plus de 32 caractères, tous les dispositifs équipés

<adresse e-mail>
+ ESPACE
+ <corps du texte>

de la plate-forme série 60 (2.6, 2.8, 3.0, 3.1) ne peuvent plus recevoir d'autres sms ou mms ; quant aux versions 2.6 et 3.0, elles se bloqueront immédiatement après le premier sms, tandis que les versions 2.8 et 3.1 se verrouilleront après avoir reçu 11 de ces messages. Pour les versions 2.8 et 3.1, après avoir reçu le onzième sms mal formaté, un message de warning s'affiche dès la réception d'un autre sms (même sain).

LES NOKIA A RISQUE

Si vous n'êtes pas sûr d'avoir une deterS60 3rd Edition, Feature Pack 1 (S60 3.1) : E90 Communicator, E71, E66, E51, N95 8GB, N95, N82, N81 8GB, N81, N76, 6290, 6124 classic, 6121 classic, 6120 classic, 6110 Navigator, 5700 XpressMusic

S60 3rd Edition, initial release (S60 3.0) : E70, E65, E62, E61i, E61, E60, E50, N93i, N93, N92, N91 8GB, N91, N80, N77, N73, N71, 5500, 3250

S60 2nd Edition, Feature Pack 3 (S60 2.8) : N90, N72, N70

S60 2nd Edition, Feature Pack 2 (S60 2.6) : 6682, 6681, 6680, 6630

Ce message prévient l'utilisateur que l'espace mémoire est plein, même si le dossier qui contient les messages en réception est vide. Une anomalie qui devrait déjà éveiller les soupçons de l'utilisateur.

Le redémarrage du téléphone portable ne résout malheureusement pas le problème, car il sera certes en mesure de recevoir à nouveau les sms, mais ces derniers seront morcelés en plusieurs parties dont seule la première sera reçue. En outre, le téléphone continuera d'afficher le message d'avertissement du fait de l'absence de mémoire. En redémarrant à nouveau le téléphone, la seconde partie du message sera reçue et, s'il en existe une troisième partie, alors elle sera reçue elle aussi au redémarrage suivant, etc..

:: Comment cette attaque est-elle réalisée ?

Pour générer l'attaque, pas besoin d'un hardware particulier : il suffit d'un mobile ou d'un modem qui supporte les commandes AT selon le standard 3GPP TS 27.005. Vous pouvez justement utiliser l'un des Nokia touché par ce problème ou un vieux 6310i, qui dispose même d'une option dédiée dans le menu qui configure automatiquement l'envoi du message en tant qu'e-mail. Il suffit ensuite de connaître le numéro associé à la carte sim insérée dans le téléphone portable "vérolé" et d'envoyer le message d'attaque.

:: Comment se défendre ?

Côté utilisateur, impossible de résoudre le problème car il s'agit d'un ver qui affecte le firmware. Tant que Nokia ne délivrera pas de nouvelle version pour chaque modèle concerné, la faille restera ouverte et vu le nombre de terminaux en jeu, elle ne sera certainement pas colmatée d'ici peu. On a appris que Nokia travaillait avec les opérateurs de téléphonie mobile pour demander un blocage sélectif de ce type de message sur leur réseau. Certains ont accepté (comme H3G - Autriche), mais pas tous. Le filtre est appliqué sur les messages qui présentent le TP-PID "Internet Electronic Mail" et une adresse e-mail composée de plus de 32 caractères. Ce blocage agit également sur les mms, dès lors que le signal de leur réception arrive par sms.

Pour rétablir le bon fonctionnement du téléphone, seul l'hard-reset semblait être la solution (obtenu en insérant le code *#7370# à partir du mode de base). Par chance, un outil gratuit est désormais disponible. Distribué par Fortinet (www.fortiguardcenter.com/mobile/cleanup.html), il permet de retirer les sms malveillants déjà reçus (que vous ne pouvez pas voir) et de bloquer l'arrivée de nouveaux si l'application est en cours d'exécution. Nous vous conseillons donc d'installer cet outil dès que possible, et d'effectuer un scan complet de votre téléphone.

TOUS LES MEILLEURS SOFTWARE

100% utile

HACKERS MAGAZINE.FR

675 MB FREE!

100 PROGRAMMES INCONTOURNABLES

HACKER WEBMASTER

COMMENT CRÉER DES SITES INVIOLABLES

EN KIOSQUE

BELGIQUE/LUXEMBOURG: 2.4 € - CANADA: 3.25 $
SUISSE: 4 CHF - TOM: 490 CFP - DOM: 2.5 € - MAROC: 25 MAD