PIRATAGE - HACKING - VIRUS- CARDING - PHREAKING - WAREZ

ZATAZ

ZATAZ

N° 9

HACKERS & PIRATES MAGAZINE

M 05129 - 9 - F: 2,00 € - RD

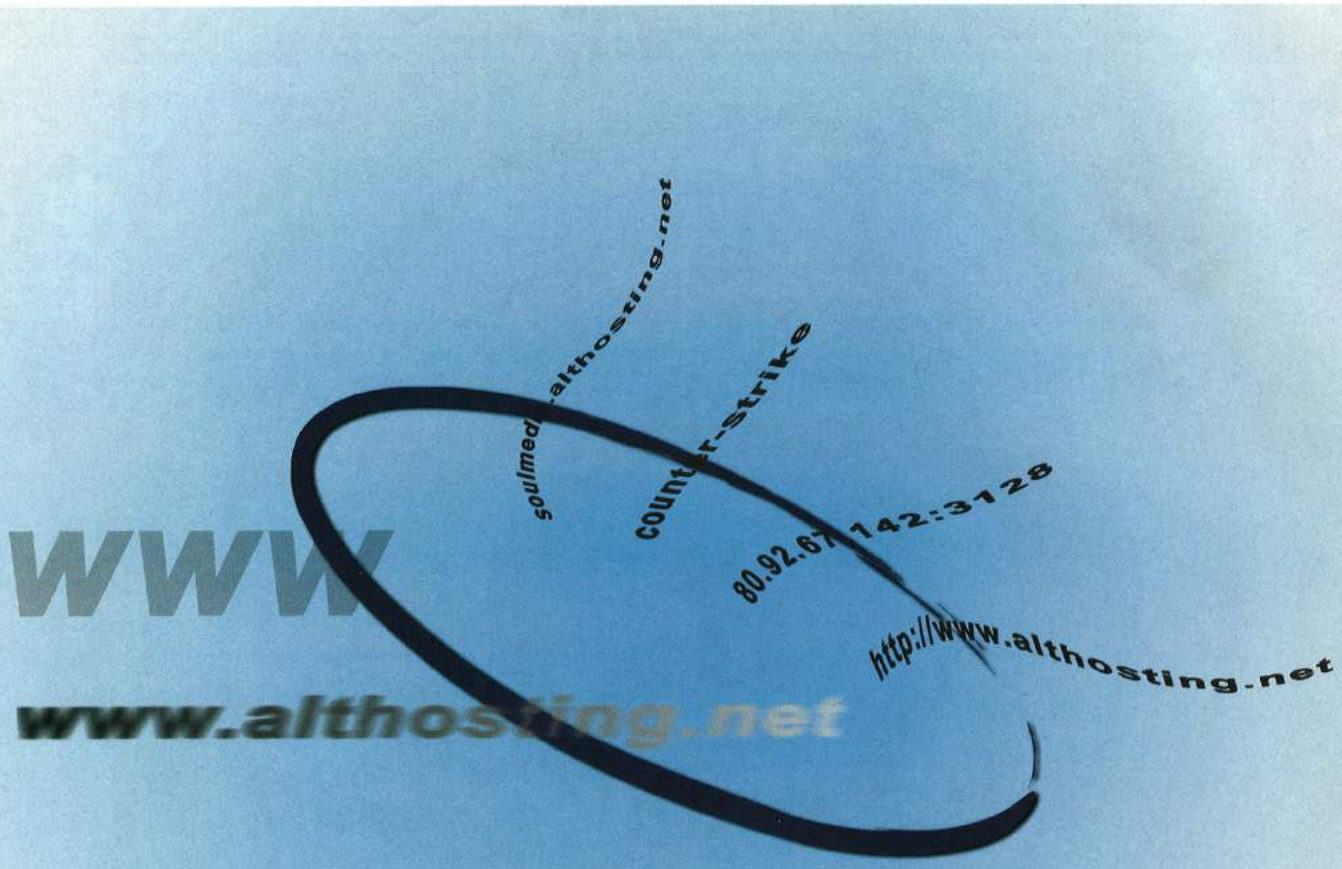
Bimestriel - Belgique : 2,3 Euros - Suisse : 4 CHF

Special nouveautés

CONFIDENTIEL

Piratage satellite
dossier special warez
Tout sur la crypto
Le buffer Overflow
Les news du hacking
et beaucoup plus...

CONFIDENTIEL



Vos solutions d'hébergements avec

Althosting.net

www.althosting.net

Althosting vous propose un large panel de solutions d'hébergements et de créations

* Serveurs dédiés.
* Serveurs mutualisés.
* Serveurs de jeux CS
* Hébergements de sites
* Créations multimédias
* Baie, Housing
* Configurations et mises à jour de vos serveurs

Althosting
Solutions d'hébergements

SOMMAIRE

Incendies, canicule, l'été fut très chaud aussi du côté de l'informatique. Des failles en pagaille pour Windows ont été corrigées, pour Linux aussi d'ailleurs. Des virii, pas moins d'une quarantaine, ont pointé le bout de leurs bits. Vous comprenez pourquoi se protéger est plus qu'indispensable pour cette nouvelle rentrée scolaire.

Une année scolaire 2003/2004 qui s'annonce chargée côté traque aux pirates et amateurs de P2P. Les associations de protection des maisons de disques et des éditeurs de films ont bien l'intention de taper fort, très fort. Comme nous d'ailleurs, encore une fois, dans ce 9ème opus de ZATAZ Magazine. Comme vous le verrez dans le sommaire : encore du gros, du bon, de l'inédit. Pas question de jouer aux hackers, encore moins aux pirates. Juste devenir des utilisateurs sensés et maîtres de leur destin numérique.

De la culture, on n'en a jamais trop avec l'auteur d'une BD traitant des pirates informatiques. De la culture, toujours, avec une réalisatrice de film qui s'est penchée sur l'hacktivisme. On a été aussi jeter notre oeil dans les cellules de la C.C.U. belge, les cyber policiers belges. On termine enfin avec le plan complet de ce réseau pas comme les autres, du producteur de warez aux consommateurs. A dévorer aussi, l'interview d'un professionnel de l'accès à la télévision à péage. Son métier, protéger les chaînes numériques des pirates. Pour finir, une nouveauté ZATAZ Magazine, eh oui, encore. Nous vous proposons de découvrir dans chaque numéro de ZATAZ Magazine Nosman, le roman d'un jeune auteur français qui raconte une histoire de hackers et de pirates.

Voilà un numéro tout chaud, bonne lecture.
Damien Bancal - taz@zataz.com

Abonnes-toi page 30
et rejoins la communauté ZATAZ !

Zataz à la radio !

Saviez-vous que ZATAZ Magazine diffuse aussi de l'actualité en audio et ceci totalement gratuitement ? Nous proposons chaque jour sur Fréquence 3, Radio Micro onde, Station Fm et radio Quebec les dernières news du moment. Si vous avez, vous aussi, une radio FM ou Web, n'hésitez pas à nous contacter par mel.

Zataz Magazine : 61, rue Jouffroy d'Abbans, 75 017 Paris. Fax: 01.40.53.86.44 E-mail : mag@zataz.com, web : www.zataz.com
Chef de la rédaction : Damien Bancal
Ont collaboré à ce numéro : Eric Romang, Christophe Schleypen, Benoît Guignard, Antoine Santo, John JEAN, Yann Busnel, Mathieu Spolix.
Correspondants : Nita et Ngyuen (Hong-Kong), Nihiatu (Dheli, Inde), Guillaume, Sam et Lucile (USA), Jeff et David - Correspondant (Tel-Aviv, Israël)
Conception graphique : Tomahawk Studio (thx Brigitte!) Impression : Léonce Deprez, Béthune Distribution France : NMPP - Belgique : AMP
Commission paritaire : 0707 T 81854 Dépôt légal à parution
Service des ventes : Distrimédias, tél. : 05.61.72.76.72 - fax : 05.61.43.49.50
Directeur de la Publication : Charles Daleau
Editeur : Mediastone, 61 rue Jouffroy d'Abbans 75 017 Paris . Siret : 422990015200019 - Code APE : 221E

Petite vérole

La jeune codeuse belge Gigabyte refait parler d'elle. Cette "virusmaker" vient de sortir un code viral nommé Coconut. Le virus cache un jeu, et pas le contraire pour une fois. L'idée, c'est de balancer des noix de coco sur deux personnages. L'un d'eux n'est autre que le pirate belge Red Attack, trublion numérique flamand qui avait défrayé la chronique judiciaire par deux fois il y a quelques mois, et un expert antivirus officiant pour Sophos. Le jeu consiste donc à faire des points en lançant les noix de coco. Chaque point correspondant à... l'infection d'un dossier de la machine de la victime. Le virus, écrit en C, se cache d'abord sur le disque dur sous le fichier coconut.exe et sous le nom de mail.vbs. La petite dame a eu l'idée - on n'en attendait pas moins de cette trasheuse - d'un ver en VBScript qui vole les informations des carnets d'adresses pour expédier coconut.exe à d'autres victimes. Pour rappel, Red Attack était un pirate belge qui a été arrêté en 1999 puis en 2001. Frank Devaere avait annoncé être capable de pirater la Général de Banque ainsi que le fournisseur d'accès internet belge, Skynet, filiale de Belgacom. La Belgique n'ayant pas de loi, il ne sera pas condamné. Elle s'occupera de nouveau de son cas en 2001 après de nouvelles bêtises numériques. http://www.zataz.com/zatazv2/news.php?id=684

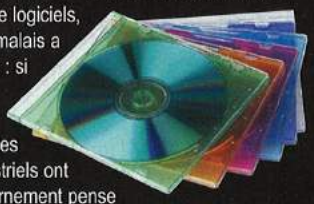
Site du gouvernement américain, cache à mp3

La police britannique a mis la main sur un garçon de 18 ans qui avait la fâcheuse habitude de cacher des mp3 pirates sur les serveurs internet des autres. Après une plainte du ministère de l'Energie Us, la police londonienne a traqué le pirate et lui a mis la main dessus. L'adolescent a piraté 17 ordinateurs du laboratoire de recherches du ministère de l'Energie Us, basés dans l'Illinois. Comme nous vous l'indiquions il y a peu, créer des stros warez n'importe où peut entraîner de sérieux problèmes.

Téléphoner à l'oeil

L'opérateur téléphonique de la Barbade, C&W, a subi un piratage lié à un problème de configuration dans les appels téléphoniques internationaux. En tapant le code *89, plusieurs centaines de clients ont pu ainsi téléphoner gratuitement. Le coût des appels n'apparaissait pas sur leur facture mensuelle. La société a perdu presque 500 000 dollars. Le porte-parole de C&W a expliqué qu'ils avaient bien l'intention de récupérer l'argent !

BAISSE DES PRIX POUR CONTRER LE PIRATAGE



La Malaisie est connue pour ses plages, son art martial - le Silat - et ... son nid de pirates en tous genres. Le taux de piratage de logiciels, films... atteint des sommets, et le gouvernement malais a donc décidé de prendre le taureau par les cornes : si les gens piratent, c'est que les prix sont trop élevés. Le ministre des finances et du commerce a donc décidé d'imposer une baisse des prix chez les éditeurs de musiques, films et logiciels. Les industriels ont proposé une baisse de 23 à 25 %, mais le gouvernement pense que ce pourcentage n'est pas encore assez fort. « Nous examinerons leurs propositions, mais si les prix sont encore trop élevés, nous déciderons des prix nous-mêmes » dixit le porte-parole du gouvernement malais. Les majors ont deux semaines pour soumettre leurs propositions. Nous vous expliquions en mai dernier, comment le gouvernement malais appelait au boycott des cds de musique ou des DVD de films pour faire baisser les prix.

MONSIEUR LE PRÉSIDENT

Etranges tableaux financiers sur le site du musicien Moby. Alors que l'on peut s'attendre à voir le dernier album du roi de la techno danse tagadatsointsoin, on se retrouve plutôt avec 4 tableaux traitant de la politique des trois derniers présidents des Etats-Unis. Employés, déficits... on peut apprécier le rase-mottes du dernier, le petit junior, G.W. Bush. Une forme de message politique de Moby. Chapeau !

BAMBI, FANS, MÊME COMBAT ?

Le roi de la pop, Mickael Jackson, a déclaré dernièrement dans la presse US qu'il ne pouvait pas supporter de savoir que des « fans » de musique, même pirates, allaient finir en prison. « Il n'est pas bien de télécharger, mais je doute que la réponse à ce problème soit la prison ». Bambi se référait à un projet de loi du Congrès américain, qui transforme le téléchargement des mp3 en crime fédéral pouvant entraîner des peines de prison.

BIEN VU !

Deux japonais de 52 et 34 ans ont été arrêtés par la BAC parisienne, la brigade anti-criminalité, fin juillet. Les deux compères venaient de faire un achat de 5 000 euros de montres dans une boutique de luxe du 6e arrondissement. D'habitude, les japonais, ils sont plutôt reçus avec des fleurs, mais pas ceux-là ! Il faut dire aussi que la police a trouvé 3 faux passeports et 23 cartes bancaires piratées. Chose cependant intéressante, l'achat a bien été validé avec l'une des C.B. Le vendeur a juste eu un doute et a téléphoné à la police.

RADIO GAGA !

ZATAZ Magazine diffuse ses actualités sous forme de modules audio de 2 minutes. Depuis septembre, 14 radios, dont 2 FM, diffusent nos news. Si vous aussi vous avez une radio et que vous souhaitez profiter de cette rubrique, n'hésitez pas à nous contacter.

MP3 EN PRISON

Le producteur Utopia Entertainment vient d'attaquer en justice la prison de Claiborne Parish, USA, pour piratage de mp3. Cette maison de disques a découvert que 3 de ses titres étaient distribués au sein de cette prison dans une liste de 330 morceaux d'albums pirates. Utopia Entertainment n'a pas perdu le nord et demande 150 000 dollars de dommages et intérêts.

BON PLAN

Les 9, 10 et 11 octobre 2003, à Marseille, plusieurs milliers de graphistes, développeurs, joueurs, utilisateurs et aficionados des outils de Macromédia, se retrouveront pour participer à la première Flash Parade organisée par le premier MMUG Flash (Macromédia User Group) français : Vision Flash. Durant 72 heures, sur plusieurs sites de la cité phocéenne dont le pôle Média Belle de mai, vont se dérouler : les Flash 2Days (conférences-ateliers ouvertes à tous) - Les Flash Conf (conférences grand public) - La Flash Tonight (nuit de projection, d'animations Flash et de courts-métrages interactifs avec le public) ou encore la Flash Games (conférences, concours de développeurs de jeux et concours de joueurs). Le défi de la Coupe América servira de fil conducteur pour les centaines de développeurs et de joueurs qui s'affronteront pour inventer du sens, des images, des animations, des jeux, autour de la mer et des bateaux. http://www.flash-parade.com/

BON PLAN 2

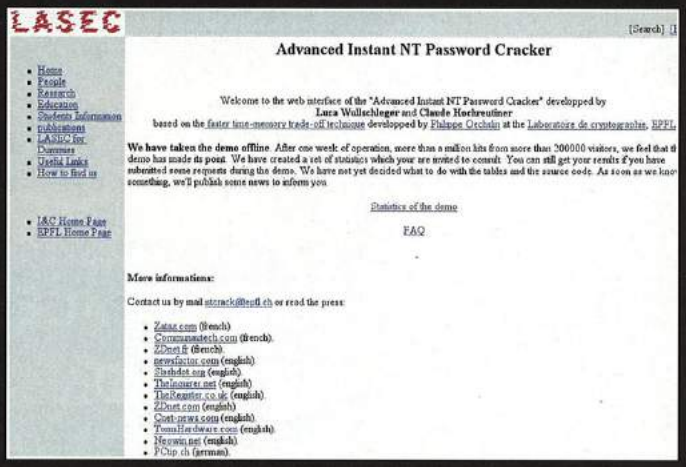
Des étudiants de la fac de Dunkerque organisent au mois d'octobre une conférence sur les logiciels libres. Des rendez-vous qui seront retransmis sur Calais, Boulogne et Dunkerque via la visioconférence.
http://www.cyberlx-littoral.fr.st

JEU SANS FRONTIÈRE

Le Japon a annulé un concours de piratage prévu au moins d'août. Le ministère de l'Economie, du Commerce et de l'Industrie, avait projeté les 11 et 12 août un concours nommé « Security Koshien », devant favoriser l'étude et l'expertise informatique parmi les lycéens et les étudiants du pays. Le concours demandait à des équipes de trois étudiants de pirater les systèmes informatiques des adversaires, tout en protégeant leur propre serveur. Le porte-parole du ministère, Takashi Kume, a expliqué que cette annulation était due au nombre important de contestations. Au japon, un pirate informatique peut être condamné à 1 an de prison et à 500 000 yens d'amende, soit quelque 4 200 euros.

JOHNNY ENGLISH

Une chaîne de supermarchés du Royaume-Uni, Tesco Market, a admis avoir évalué la technologie controversée qui permet de suivre à la trace un produit équipé d'une puce. Dans ce magasin, une personne qui a acheté des lames de rasoir Gillette Mach3 a été photographiée. Une association US a constaté que les étiquettes espionnes, cachées dans la boite à lames, déclenchaient une caméra de surveillance quand un paquet était retiré du rayon. Une seconde caméra photographie de nouveau l'acheteur et le personnel de sécurité compare les deux images. Voilà une méthode intrusive imparable !



CRACK EN 5 SECONDES CHRONO

Des étudiants de l'Ecole Polytechnique Fédérale de Lausanne, Claude Hochreutiner, Luca Wullschleger et Philippe Oechslin, viennent de terminer un projet de semestre au LASEC (Laboratoire de sécurité et de Cryptographie, ndlr) sur le crackage des mots de passe Windows (LanManager hash, ndlr) basé sur une méthode probabiliste. Ils ont réussi à cracker n'importe quel mot de passe alphanumérique (chiffre + lettres, ndlr) de n'importe quelle longueur et cela en... 5 secondes ! Ce qui est 6 000 fois plus rapide que n'importe quel brute force comme LC4, John the Ripper, Lopht Crack... L'EPFL semble être un vrai nid de talents. Les scientifiques de cette école avaient réussi en fevrier dernier la mise en avant d'une faille du protocole SSL, Secure Socket Layer, qui était réputé inviolable.
http://lasecpc13.epfl.ch/ntcrack

2 000 ANS DE JUGEMENT

Selon la Fondation EFF il y a, aux Etats-Unis seulement, 60 millions de personnes qui partagent des fichiers via le P2P. Si la RIAA souhaite poursuivre en justice les internautes cités (l'association l'annonce à grands coups de communiqués de presse), cela va lui prendre 2 191 années, à la condition qu'elle dépose 75 plaintes par jour. Une chose est certaine : ceux qui vont s'enrichir ne sont pas ceux que l'on croit, en tout cas pas les musiciens. On va plutôt pencher pour les avocats !

UN PETIT SÉVICE POUR LA ROUTE ?

Conformément aux nouvelles lois traitant de la sécurité des Etats-Unis, United States homeland security laws, toutes les écoles américaines doivent enregistrer leurs étudiants étrangers dans une base de données nommée SEVIS (Student and Exchange Visitor Information System). Il parait que le système est tellement au point qu'il est déconseillé aux étudiants de rentrer chez eux durant leurs études.

MORT ANNONCÉE

La société Elaborate Bytes vient de faire savoir - pour le moment officieusement - qu'elle ne sortira plus de nouvelles versions de CloneCD, logiciel qui porte bien son nom vu qu'il clone les cds qui pourraient être protégés contre la copie. Une fin annoncée, en raison de nouvelles lois allemandes plus que restrictives sur le copyright. A partir du mois d'août, CloneCD et CloneDVD deviennent des logiciels interdits.
« 3 ans de prison, on préfère éviter les frais » dixit l'un de nos contacts chez Elaborate.

LES CHASSEURS DE PIRATES DONNENT DES COURS

Une nouvelle campagne, plus douce, contre le piratage de films sur internet va être lancée ce jeudi aux Etats-Unis. Les studios demandent « gentiment » dans des annonces TV et devant les cinémas, de ne pas pirater de films via internet. Les publicités, ainsi que les stands devant les cinémas, vont présenter les métiers du 7ème art. L'idée étant d'informer sur les métiers qui pourraient disparaître à cause du piratage : maquilleurs, preneurs de son, effets spéciaux, acteurs... La MPA (L'Association des Majors d'Hollywood) a aussi développé un programme scolaire sur les droits d'auteurs. Nommé « Digital Citizenship » ce programme couvre l'histoire du cinéma et du droit des auteurs. Un concours est même organisé pour proposer aux étudiants d'indiquer des méthodes pour contrecarrer le piratage via internet.

1984 dans le métro

Voilà qui laisse songeur. Les robots vont commencer à nous surveiller. Deux stations de métro de Londres vont tester cette semaine un logiciel nommé "Intelligent Pedestrian Surveillance System". Conçu par Sergio Velastin, son but est d'aider les surveillants devant leurs télévisions à traquer les comportements bizarres. Le logiciel est capable, parait-il, de détecter une tentative de suicide, un colis suspect, un tagueur... 60 caméras vont servir à ce Big Brother urbain.
http://www.newscientist.com/news/news.jsp?id=ns99993918

Portes ouvertes bancaires

Voilà qui n'est pas courant. Un gros problème de sécurité concernant une banque française. L'un de nos lecteurs souhaitant consulter son compte en ligne, a tapé le mot-clé de sa banque dans le moteur de recherche « Google ». La banque en question est le Crédit Agricole Sud Méditerranée. La première réponse qui a été donnée par le moteur de recherche a donné accès au code jsp de la page. En parcourant cette page, il était possible de tomber sur des requêtes sql, qui concernaient des bases Oracle. Après le passage par les mains d'une dizaine de salariés de cette banque, nous sommes enfin tombés nez à nez avec le responsable. Le site a été corrigé dans l'heure qui a suivi notre appel.

Anti-spyware gratuit

La société britannique PestPatrol propose un logiciel qui permet d'éradiquer Spywars et autres espions numériques. Pour promouvoir son logiciel, cette entreprise met à disposition son traqueur d'espions via son site internet et un service nommé « PestScan ». PestScan est un logiciel de sécurité qui va permettre de chercher et effacer les espions de votre machine. Seul inconvénient, à notre goût : il faut télécharger quelques petits composants ActiveX dans l'ordinateur d'un utilisateur.
http://www.pestscan.com/

Delete !

La deuxième grosse société internet suisse, Freesurf de Sunrise, a eu une panne qui vient de laisser sur le carreau 400 000 clients. Le service d'e-mail de Freesurf et de Weboffice de Sunrise est H.S. depuis lundi dernier. On ne sait pas encore comment, ni pourquoi, les serveurs qui hébergeaient les courriers électroniques des clients ont été détruits. Pour une fois, ceux qui utilisent Outlook sont les seuls à ne pas subir ce problème, le logiciel gardant en mémoire les mels rapatriés avant le crash.
(Merci à Luder)

CASQUETTE ZATAZ

Vous avez été très nombreux à nous la demander, c'est le moins que l'on puisse dire, avec pas moins de 2 758 mels à ce sujet. Nous avons donc décidé de vous faire plaisir. Nous venons de recevoir les premières casquettes ZATAZ Magazine. Elles sont beiges, de marque Oakland, avec le logo ZATAZ brodé.
Elles sont vendues 19 euros. Pour en savoir plus, envoyez un mel à la rédaction.

NERO EFFACE VOTRE H.D.

Le magazine en ligne allemand Pcwelt, annonçait que Nero 6 contenait un défaut qui supprimait le contenu de votre disque dur. Les codeurs de ce logiciel de gravure avaient juste oublié de limiter la fonction qui gère le dossier temporaire. Nero effaçait ce dernier et continuait sa route en effaçant l'ensemble du disque dur.
La version 6.0.011 corrige ce fâcheux bug.

SOUS SURVEILLANCE !

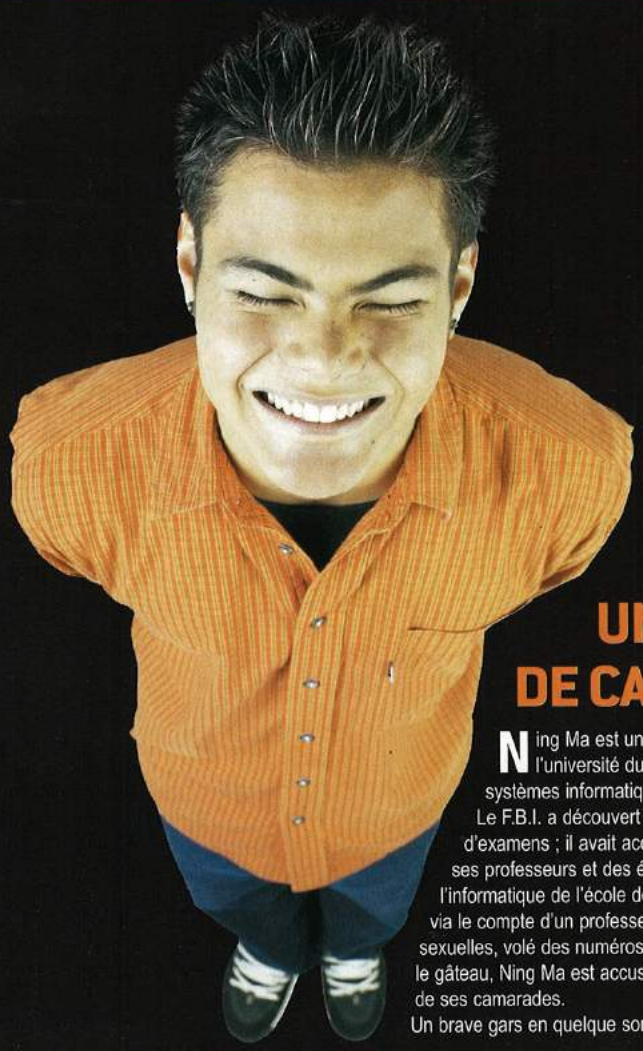
La police fédérale australienne est en pleine discussion avec les fournisseurs de courriers électroniques gratuits, dans l'espoir de mettre en place des méthodes pour tracer plus facilement pirates, escrocs ou pédophiles. Certains ont même avancé la fermeture pure et simple des services mels gratuits.
http://www.iia.net.au/cybercrime_code_v2.doc

MICROSOFT PIRATÉ

Le site Microsoft.com a disparu complètement de l'Internet vendredi 1er août. Par deux fois au moins, le site a été attaqué par un Déni de service Distribué, un DDoS. En gros, vous prenez plusieurs centaines de machines, (ici on pourrait penser à plusieurs milliers), et vous les faites discuter en même temps avec le même serveur. Radical, ce dernier plante. Un peu comme si toute la planète vous téléphonait en même temps. L'attaque, confirmée par le porte-parole de Microsoft Sean Sundwall, a empêché dans la foulée tout téléchargement et installation de patches durant plusieurs dizaines de minutes.

ON NOUS AURAIT MENTI ?

Le magazine hollandais Pc Active vient de conclure un test de 2 ans ayant pour but de contrôler l'intégrité des CD-Roms vendus dans le commerce.
Ils ont démontré que les promesses des packaging et autres services marketings annonçant une durée de vie de 10 ans et plus étaient faux.
Les données enregistrées il y a 20 mois sur ces CD-Roms sont ensuite devenues illisibles.
Les disques testés étaient pourtant tous de grandes marques.
Souvenez-vous, il n'y a pas si longtemps, on vendait le CD-Rom comme un support plus résistant qu'une cassette ou un vinyle !



UN AMOUR DE CAMARADE

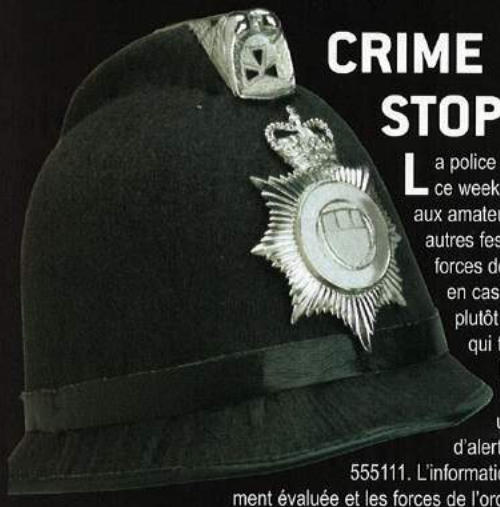
Ning Ma est un chinois de 24 ans, étudiant en troisième cycle à l'université du Michigan. Il vient d'être arrêté pour piratage des systèmes informatiques de son école.
Le F.B.I. a découvert que ce brave garçon avait obtenu les copies d'examens ; il avait accédé aux comptes des courriers électroniques de ses professeurs et des élèves. Il avait caché un peu partout dans l'informatique de l'école des sniffers, envoyé de faux courriers électroniques via le compte d'un professeur à un étudiant, lui proposant des relations sexuelles, volé des numéros de cartes bancaires de professeurs, et, cerise sur le gâteau, Ning Ma est accusé d'avoir annulé l'entretien d'embauche de l'un de ses camarades.
Un brave gars en quelque sorte !

MÊME PAS CHER !

Etrange produit que celui présenté par la boutique Online Marcopoly. Pour 1 euro il était possible d'acquérir une Clé USB MP3 32 Mo transformable en un lecteur/baladeur pouvant également stocker toutes les données comme un disque dur amovible !
Vu que le prix affiché est obligatoirement celui qui doit être appliqué, voilà une très bonne affaire ! Allez, nous ne sommes pas malhonnêtes !
Nous avons alerté Marcopoly qui a corrigé son erreur, sans toutefois prendre la peine de nous remercier de les avoir prévenus. Charmant...

EXPLOIT PS2

Un code, nommé HOP, vient d'être publié sur internet et permet de faire tourner un logiciel sur la PS2 de Sony sans puce underground. Comme vous devez le savoir, pour utiliser des jeux imports ou des copies qui n'ont que de sauvegarde que le nom, les consoles de jeux ont besoin de modchip, une puce à intégrer dans la console. La Xbox a été la première a voir débarquer un code qui permettait de se passer d'une puce. La faille avait été découverte via le jeu 007 under fire. Le système de codage/décodage, n'avait pas été... codé. Aujourd'hui, c'est au tour de la Playstation 2 de Sony de voir débarquer sur le réseau des réseaux un code qui permet de se passer d'une puce pour faire tourner un programme. D'après son auteur, 0xd6, il suffit de rajouter au jeu le code HOP et le tour est joué.



CRIME STOPPERS

La police britannique a offert ce week-end la possibilité aux amateurs de concerts et autres festivals d'alerter les forces de l'ordre par SMS en cas de délit. L'idée est plutôt sympa. Une bagarre qui tourne mal, un vol, les témoins pouvaient envoyer un SMS anonyme d'alerte via le 0800 555111. L'information était immédiatement évaluée et les forces de l'ordre déployées où il était nécessaire. Le système, appelé Crimestoppers a fonctionné durant le V2003 music festival, qui était dispersé sur plusieurs sites.
Un festival sponsorisé par ... Virgin Mobile.

COMMUNICATION P2P

L'association des majors du disque canadiens, la Canadian Recording Industry Association, utilise la messagerie instantanée installée dans les outils de P2P comme KaZaa pour contacter les internautes qui mettent à disposition de la musique commerciale au format Mp3. La CRIA pense que communiquer avec les pirates est l'une des meilleure manière afin de leur faire comprendre ce qu'il risque et des dégâts qu'ils infligent aux créateurs de musique. Les associations de l'industrie du disque australien, danois ou encore allemand vont rejoindre la CRIA dans cette initiative.

IT'S A NAVY !

L'intranet de la marine militaire Us, Navy/Marine Corps Intranet, a été perturbé par un virus informatique. Une attaque combinée par le worm blaster et le dernier en date Sobig.F. L'intranet du N/MCI a quand même coûté plus de 6 milliards de dollars et est censé sécuriser toutes les communications audios, vidéos, textes de l'intranet de la Navy. A noter qu'on propose sur notre FTP, répertoire antivirus, un antidote gratuit pour contrer ce nouveau Sobig version F.

FAUX CALME

Depuis quelques mois la police suisse s'est équipée d'une section internet regroupant 8 cyberflics au sein du Service de Coordination de la lutte contre la Criminalité sur Internet, la SCOCI. Depuis janvier, cette cellule a déjà reçu 3 600 alertes provenant d'internautes. 500 cas sont signalés chaque mois, 36 cas ont visé des actes de pédophilies. Nous vous proposions dans ZATAZ Magazine papier numéro 7 l'interview d'un des policiers de la SCOCI.

TON PORTABLE SUR INTERNET

Lu sur le site de la CNIL Les coordonnées des téléphones fixes et mobiles vont pouvoir désormais figurer dans un annuaire universel. C'est un décret du journal officiel, paru le 6 août dernier, qui impose aux opérateurs de communiquer leur liste d'abonnés à toute personne souhaitant éditer un annuaire universel. France Télécom devra mettre à disposition gratuitement à ses abonnés ce type d'annuaire dans chaque département de plus les abonnés pourront demander à leur opérateur de faire figurer leur adresse électronique et leur profession.
Si vous ne souhaitez pas figurer dans ce futur outil à spameur, il vous faudra passer en liste rouge, qui dans la foulée n'est plus payante.

DEMO'NIAK

Comme chaque mois nous allons faire un petit tour du côté des créatifs de l'underground informatique, les démomakers. Dernières productions à vous exploser les neurones et les prochaines dates des Démos party. Dans ce numéro, nous allons visiter les sites internet de groupes de démomakers français.

ALGORYTHM ABSTRACTION

Un groupe de démomaker français qui semble aimer l'humour ! « Nos productions sont aussi rares et demandées que les montres à aiguilles sans aiguilles. Si vous avez compris ces quelques lignes vous êtes fin prêt pour rentrer dans la philosophie d'AAbs. » A voir, pour ceux qui sont sous Linux le premier projet de cette team, une démo en OpenPTC nommée Sproutch the Mosquito. http://www.aabs.fr.st/

BLA BLA

Même si ce groupe n'existe plus, vous pouvez toujours vous jeter sur leurs productions. Atari, PC, de quoi vous en mettre plein les yeux.

http://blabla.planet-d.net/Demos.php3

ESPRIT !

Le groupe BMK zone ne propose pas à première vue beaucoup de productions, mais vous allez tout de suite comprendre l'esprit qui fait un bon groupe de démomakers. « Attention, nous ne sommes pas une start-up ; néanmoins, si des investisseurs technodébiles et bedonnants veulent nous arroser de millions de francs, pas de problèmes, on les boira à leur santé (c'est comme ça que marche une start-up non?). (...) Vous pourrez vous bidonner, par exemple, avec la BMK Tv. http://www.bmkzone.com/

BOMB

L'une des grosses références demomakers dés années 90. Le groupe Bomb! savait sortir des démos qui savaient vous scotcher à l'écran. L'un de leur graphiste, MADE, génie de la palette depuis l'époque de l'Amstrad CPC, savait rendre encore plus démentielle une production via ses dessins.

http://bomb.planet-d.net/

UN ARRIÈRE GOÛT DE VACANCES

Beau, voilà le mot qui nous est venu à l'esprit à la vue de l'intro nommé « Egypt ». Vous allez visiter les pyramides via une intro en 3cd ne pesant à peine que 24 kilos octets. Pour ceux qui touchent un peu au code, la petitesse de la programmation montre une certaine dextérité du démomaker italien nommé Ninja Killer. La musique est signée par Kenet. http://web.tiscali.it/hiforce/3gypt/

ECLIPSE

Quand les démomakers français se lancent dans le jeu vidéo, ca donne Eclipse Game. Vous pourrez trouver sur ce site 5 productions du groupe Eclipse. Un pac-man, un shoot'n up ... Vous trouverez aussi des démos et intros datant de la fin des années 90. Old shool powa !

http://www.eclipse-game.com/htm/main-frame.htm

JUST FOR FUN

Voilà un autre groupe français qui porte bien son nom. Sur JFF vous y trouverez des intros, démos old school dont la très chouette SOFTWORLD. A noter d'ailleurs pour ceux qui veulent se lancer dans la démo, le groupe just For Fun propose le code source de la Softworld démo. De quoi pouvoir vous faire les griffes.

http://www.j-f-f.net/

JAMAIS DEUX SANS TROIS

Nous devions nous rendre à la BZH party qui s'est tenue en Bretagne cet été ! Manque de temps et nous voilà leur posant un lapin. On a aussi, semble-t-il, raté une sacré party entre fans de l'esprit Old School. On en peut que vous inviter à visiter le site Web de cette démo party ou vous y trouverez images, 3d, musiques et bien sur démos à télécharger. http://bzhparty.free.fr

L'agenda des demomakers

- **Nom : Abstract 2oo3**
  Date : 6/7 septembre
  Lieu : Pologne
  Site : http//fabstract.nahkolor.net
- **Nom : XzentriX**
  Date : 12/13/14 septembre
  Lieu : Allemagne
  Site : http://www.xzentrix.de
- **Nom : HamsterParty**
  Date : 27 et 28 septembre.
  Lieu : Villers les Nancy, France
  Site : http://woodtower.free.fr%2fhp
- **Nom : Bcn party'11**
  Date : 31 oct. 1/2 nov.
  Lieu : Barcelone, Espagne
  Site :http://www.www.bcnparty.org
- **Nom : Compusphere 14**
  Date : 28/29/30 novembre
  Lieu : Gothenburg, Suède
  Site : http://www.compusphere.org

Tout l'univers de Maurice sur Internet

LE SITE DU SORCIER DES ONDES

MauriceRadioLibre.com

LE BON, LA BRUTE ET LES TRUANDS

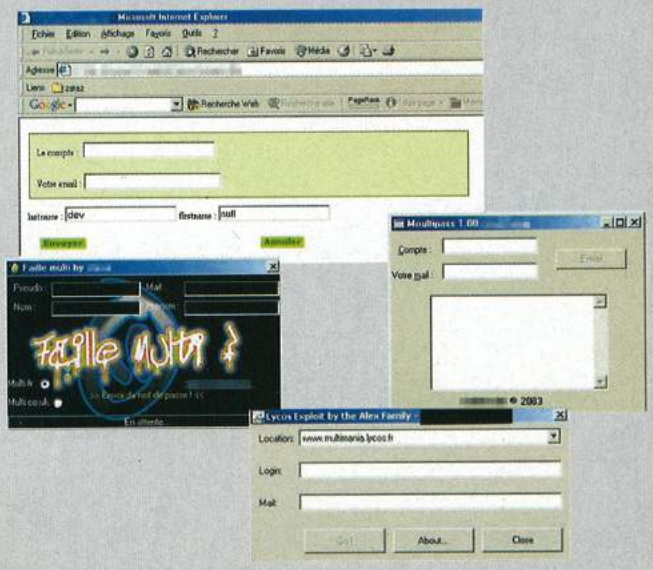
EN MAI 2003, UNE ÉTRANGE INFORMATION EST PARVENUE À NOS OREILLES. IL ÉTAIT POSSIBLE D'ACCÉDER À N'IMPORTE QUEL SITE HÉBERGÉ CHEZ LYCOS. NOUS AVONS CHERCHÉ, ET TROUVÉ.

MOT DE PASSE ET CODE SOURCE

Nous vous expliquions dans Zataz 6 comment une bête faille permettait d'accéder aux répertoires de sites hébergés chez Lycos/Multimania. Rien de méchant, sauf que ce bug permettait aussi d'accéder aux codes sources des pages php et dans le pire des cas, aux logins et mots de passe de bases de données SQL. Ce problème a été corrigé après notre alerte. Cependant, très vite, nous nous sommes rendu compte qu'un autre problème persistait. Plus grave, car la rumeur laissait entendre qu'avec un simple mel il était possible de récupérer login et mot de passe d'un site web Multimania.

EXPLOIT, CODE, .EXE

Selon la rumeur, la nouvelle faille permettait d'accéder à n'importe quel compte web Multimania, et de manière radicale. Pas de programmation, de bug de language. Une faille universelle et sans limite. Une faille qui permettait un renvoi de logins et mots de passe web, mais aussi Ftp du compte Multimania. Le fonctionnement de cette faille était somme toute très "simple". Il reposait sur un défaut de programmation. Pour l'utiliser, les pirates devaient poster des requêtes HTTP (comprenez de simples informations dans une url). Cette faille nous paraissait invraisemblable, mais elle semblait effectivement exister au vu des démonstrations qui nous avaient été faites à l'époque sur nos propres comptes Lycos. Cette même erreur de programmation existait sur toutes les versions de Lycos. Soit plusieurs millions de sites web prêts à être frappés par n'importe quel pirate en mal de reconnaissance. Il nous a suffi d'imaginer les conséquences désastreuses qu'aurait pu engendrer la publication d'une telle faille dans tous les forums de pseudo-hackers à travers le monde. Nous avons donc alerté Lycos France rapidement. L'équipe de cette entreprise a été plus que réactive. Quelques minutes après notre alerte, les pirates pouvaient retourner d'où ils venaient, soit vers le néant. Nous nous étions posé la question de savoir quelle aurait été la possibilité pour un pirate d'automatiser complètement la tâche, pour un défacement de masse des pages web via un programme récupérant sur un compte mail muni d'un POP, certains champs du mail reçu - à savoir login et passe ftp - et que ces deux valeurs soient transmises en temps réel sur un logiciel ftp. Les conséquences auraient pu être désastreuses. Eh bien, vous auriez eu raison de le penser ! Nous avons découvert lors de notre enquête sur cette faille que des codeurs avaient commencé à automatiser le problème en question.



FULL-DISCLOSURE : LES POUR ET LES CONTRE

Par ce terme anglais, le full-disclosure, on entend la diffusion d'une faille, d'un exploit, donc d'un problème de sécurité informatique, afin d'avertir la société faillible et les utilisateurs des logiciels, systèmes, sites, ayant une faille pouvant mettre en danger leurs informations et leurs vies privées. Une alerte, comme on en trouve des milliers sur le site BugTraq, propriété de Symantec, se nomme advisory. Il existe deux groupes de pensée : les pour, qui veulent que soient diffusées ces alertes, et ceux qui refusent cette diffusion en pensant qu'elle sert surtout à nourrir les pirates, ce qui est honnêtement pas si faux que cela.

QUI C'EST QUI TOC !

Cette faille semble avoir séjourné pendant quelque temps dans un cadre bien fermé de releasers français, jusqu'au jour où un groupe français s'est illustré (la Alex Family), en sortant un programme open source, automatisant complètement la tâche. Ce programme d'une simplicité enfantine, ne demandait que trois informations : le pays, le login du compte que le pirate souhaitait "visiter", et le mail où Lycos devait envoyer le password. Un programme qui effectuait seul tout le processus de modification et d'envoi de mot de passe. Ce programme codé dans un esprit de "découverte" par cette team connue pour ses développements et releases open source, aurait pu se transformer en véritable arme à script kiddies. Il suffit de prendre pour exemple l'exploit de la faille WebDAV codé avec intelligence par Kralor, et exploitée par tout un groupe de script kiddies. Le problème du full-disclosure repointe le bout de son museau. A noter que nous allons découvrir pas moins de 4 autres logiciels utilisant cette faille, ainsi qu'une page html automatisant elle aussi le processus - mais dans une moindre mesure, page qui a été réalisée par un certain Ansuketor. Quand on pense que le champ d'action utilisateur face à une telle faille était quasi inexistant puisque celle-ci agit côté serveur, on peut dire que les pages persos hébergées gratuitement par Lycos ont eu chaud, très chaud.

L' Organization for Internet Safety (OIS), a présenté un projet de normalisation de processus de publication et de correction des failles de sécurité. Le but : limiter les conflits entre les "inventeurs" de failles et les éditeurs de logiciels, éditeurs comme Microsoft, Oracle, Sco, Network Associates, ISS, Guardent, Symantec... qui trônent dans cette organisation. Si on a bien tout suivi, l'éditeur a 7 jours pour répondre et accuser réception d'une faille. Si aucune réponse ne parvient à l'inventeur, ce dernier doit réécrire pour demander confirmation de réception de son premier mel. L'éditeur ajoute 3 jours dans son escarcelle « alerte ». Si les trois jours n'ont pas suffi, l'inventeur du problème doit encore attendre 30 jours avant diffusion, après que l'éditeur, lui, ait disposé d'un délai maximum de 30 jours pour effectuer l'investigation et la qualification du problème. A savoir, faille ou pas faille. Bref, avertir les utilisateurs qu'ils sont en danger 70 jours après l'avoir découvert... Autant apprendre à danser la gigue, ça sera moins long. Toujours est-il que nous avons suivi à la lettre la normalisation de l'OIS. On doute que tout le monde soit aussi patient ! http://www.oisafety.org/resources.html

PIRATAGE DE SATELLITE

AVEC NOTRE INFORMATION SUR LE PROBABLE CASSAGE DU MODE DE CHIFFREMENT SECA 2 NOUS NE PENSIONS PAS TOMBER DANS UN TEL NID DE VIPÈRES. IL EXISTE CERTES ENCORE QUELQUES VRAIS PASSIONNÉS DE RECHERCHE, MAIS FACE AUX PETITS VOLEURS À LA SAUVETTE PRÊTS À PIRATER TOUTES LES CHAÎNES DE TV, IL EST DIFFICILE DE DISTINGUER LE BON DU MAUVAIS. NOUS AVONS POUR CELA RENCONTRÉ MR X. POUR DES RAISONS DE SÉCURITÉ NOUS NE DÉVOILERONS PAS SON IDENTITÉ. MAIS ACCROCHEZ-VOUS, SES RÉVÉLATIONS SONT SANS DÉCODEUR.

Qui êtes-vous ?

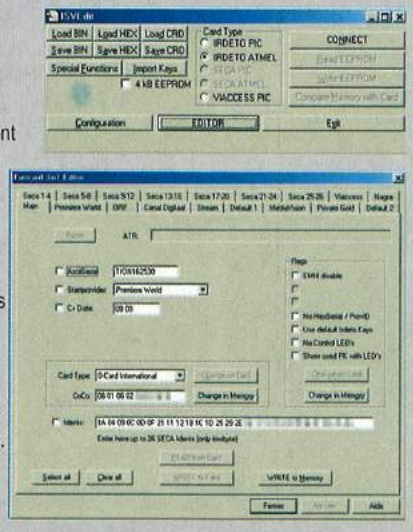
36 ans, parisien, je suis ingénieur en informatique, et je bosse depuis 14 ans (déjà). J'ai commencé par 6 ans de développement pour des applications militaires, et depuis je travaille dans la TV numérique où j'ai "sévi" chez plusieurs fabricants. Depuis 6 ans, dans le domaine de la télévision numérique, je me suis spécialisé dans la partie contrôle d'accès, c'est-à-dire la partie qui fait que le décodeur ne fonctionne que si on y insère une petite carte à puce, et qu'en plus on paye son abonnement mensuel.

On parle de plus en plus de piratage satellite... Cela fonctionne comment, dans les grandes lignes ?

Alors, il y a beaucoup de formes différentes de piratage :
Le piratage des abonnements. Cela consiste à remplacer la carte officielle par une carte à puce pirate (basée sur les mêmes composants que les tristement célèbres Yescard, ndlr). C'est en diminution, car parmi les 5 grands fabricants de cartes de contrôles d'accès, 3 d'entre eux qui étaient crackés il y a deux ans ne le sont plus. Il n'en reste donc aujourd'hui qu'un seul réellement piraté, et encore, pas sur tous ses systèmes. Vient ensuite le piratage du soft décodeur. Certains fabricants indélicats développent eux-mêmes le soft utilisant la carte à puce embarquée dans le décodeur, en plus bien évidemment, de ne pas payer les royalties au fabricant original du soft. C'est un peu comme si quelqu'un fabriquait un logiciel permettant de lire ou écrire des fichiers Word, sans payer de royalties à Microsoft. Certains même vont mettre ensemble, dans le même décodeur, ou dans le même module de contrôle d'accès détachable, plusieurs systèmes concurrents. Mediaguard, le système permettant de décrypter Canal, ou Viaccess, celui qui permet de décrypter TPS, Irdeto qui décrypte Stream et Nagra qui décrypte les bouquets espagnols, par exemple. Toujours sans payer de licence.
Ce système est dangereux, y compris pour le consommateur qui croit avoir acheté un système universel, mais en cas d'évolution technique de l'un des contrôles d'accès, il y a beaucoup de chances pour que son décodeur ne fonctionne plus. Du court terme pour le consommateur. Une concurrence déloyale pour les fabricants honnêtes qui payent des licences et des royalties, et respectent les procédures de développement et de validation des fabricants de contrôles d'accès qui sont longues, lourdes et coûteuses. Cela permet de s'assurer du bon fonctionnement dans tous les cas, et de l'évolutivité réelle du produit.

Cette guerre Opérateur/pirate tourne-t-elle autour de la cryptographie ?

En fait, les opérateurs ne sont "que" des clients des fabricants des systèmes de protection (que l'on appelle contrôles d'accès, ndlr). La guerre des cartes crackées est donc entre ces fabricants de contrôles d'accès et les pirates. Le problème n'est pas vraiment la cryptographie, car les algorithmes utilisés ne sont pas crackables.



logiciel de lecture de carte pour satellite

Dans tous les cas de cartes pirates, l'algorithme n'a jamais été cracké, il a juste été dévoilé.

Comment se fait-il que les pirates arrivent toujours à casser ces clefs ?

Ils ne cassent pas les clefs, ils arrivent à y avoir accès... C'est très différent. En fait, dans les cartes à puce officielles, on trouve le code avec les algorithmes de cryptographie d'une part dans une rom, et les clefs qui servent à désembrouiller, dans une partie flash... Le jeu consiste donc à trouver un moyen de lire le code et les clefs. Une fois qu'ils ont le code, il "suffit" de le désassembler pour avoir l'algorithme, qui ne sert cependant à rien sans les clefs. Dans beaucoup de cas le code et/ou les clefs ont été extraits parce que les cartes n'étaient pas protégées, ou parce que les softs comprenaient des bugs. Souvent l'accès au code permet de l'analyser, de trouver des bugs dans le soft, et de tirer partie de ces bugs pour arriver à lire les clefs. Par exemple, si on parle de SECA 1, tout semble venir de la diffusion sur internet d'un binaire nommé SECAROM, qui reprenait la rom de la carte SECA 4.0... Les chercheurs ont analysé ce binaire, et trouvé pas loin d'une trentaine de failles différentes qui permettaient, par l'envoi de commandes spécifiques non prévues à l'origine dans le système, de "sortir" les clefs. Sans la publication de ce SECAROM, rien n'aurait sans doute été possible.

Vous avez dû certainement suivre l'affaire Murdock-NDS / Canal Plus Technologie ?

Oui ! Il y aurait eu, selon Canal + Technologie, un processus délibéré de NDS, qui aurait utilisé des moyens énormes (ses propres laboratoires de recherche et ses propres experts, ndlr) pour cracker ses concurrents, et arriver à lire la rom... Et qui l'aurait ensuite diffusé (le fichier SECAROM.bin auquel il est fait allusion ci-dessus, ndlr).
En fait, parmi les 5 ou 6 fabricants de contrôles d'accès qui se battent pour le marché non américain (le système US est différent, ndlr), il y en a 1 ou 2 qui ont en effet l'air d'être prêts à tout pour affaiblir leurs concurrents, y compris des procédures malhonnêtes, un non-respect de propriété intellectuelle...

On parle depuis quelques jours du cryptage SECA 2 qui serait cassé, qu'en pensez-vous ?

Je suis comme saint Thomas, je ne crois que ce que je vois. Ceci dit, il y périodiquement des rumeurs, et celles d'aujourd'hui sont un peu plus fortes que les autres. Ce qui est étrange quand même, c'est que Canal+ Technologie ait jugé nécessaire de faire en 1 an, trois versions différentes de ses cartes... La 7.0 pour l'Espagne et l'Italie, la 7.1 pour la France, et la 7.3 pour la Hollande et la Belgique. Normalement, quand un système de contrôle d'accès est fiable, on ne le fait pas évoluer aussi vite...

Aujourd'hui les opérateurs, Canal Sat, TPS, mais aussi et surtout aux USA, lancent des attaques numériques. Comment cela fonctionne-t-il ?

En fait, beaucoup de décodeurs intègrent des moteurs interactifs (Mediahigway pour Canal+, Open TV pour TPS, Ndlr), qui sont un peu comme des machines virtuelles Java, et qui permettent donc d'effectuer le même code interprété sur tout son parc de décodeurs, quel que soit le processeur que le décodeur intègre. La plupart des "contre-mesures" des opérateurs sont basées là-dessus. Ils envoient dans les airs de nouveaux programmes qui vérifient que les échanges entre les cartes et les décodeurs sont bien "normaux", et ils détectent ainsi les différences entre les cartes officielles et les cartes normales. Il y a maintenant d'autres systèmes plus intelligents, qui n'utilisent pas ces machines virtuelles, et qui sont plus efficaces. Je ne m'étendrai pas sur le sujet.

HACK AND CASH la bédé des hackers...

Elle se prénomme Aka, une jeune fille hacker qui veut venger la mort de ses amis. Elle est l'héroïne de la bande dessinée d'Alain Maindron. Nous sommes allés interviewer cet auteur pas comme les autres.

Qui est Alain Maindron ?
Dessinateur, auteur. J'ai passé la plupart de mon temps hors de France (Angleterre, Australie, USA) où j'ai travaillé pour une longue liste de sociétés diverses. Je suis en France depuis deux ans, et je découvre de nouvelles expressions comme « C'est clair » ou « j'hallucine » qui n'existaient pas quand je suis parti. Par contre, le fait que je glisse par inadvertance des mots anglais dans mes phrases ne semble plus déranger les gens comme avant :)

Pourquoi Hack and Cash ?
Hack : pour parler de ce monde parallèle, underground opposé au monde des affaires : Cash. En gros, un monde illégal versus un monde légal.

Pourquoi le sujet des hackers dans votre BD ?
Les aventuriers d'aujourd'hui ne sont pas des journalistes qui vont d'une guerre à l'autre, ou des sportifs de l'extrême, car quelque part ils ne découvrent rien. Par contre un hacker, en général, n'est pas un type sponsorisé par des sociétés, il agit généralement seul, et illégalement, même s'il ne fait pas de mal. Il faut un certain courage pour risquer de se mettre toute une société à dos. Et puis, n'est pas hacker qui veut. C'est un peu comme devenir magicien dans une fable, il y a un langage spécial qui donne accès à un pouvoir bien réel. C'est ça le truc : les hackers ont un pouvoir qu'ils prennent, ils n'attendent pas qu'on le leur donne.

Comment avez-vous travaillé le scénario ?
L'idée de hacker un site de la façon décrite dans l'album m'est venue lorsque j'apprenais à créer des sites moi-même. J'avais l'intention de créer une sorte de grand jeu sur internet en utilisant de fausses pages et de vrais sites internet. L'histoire elle-même m'est venue très vite, en fait elle s'est imposée d'elle-même. Je crois que c'est le résultat de pas mal de pensées inconscientes qui un jour font surface.

Votre héros se nomme Aka et c'est une fille, pourquoi ?
Parce que je suis un mec, j'imagine. On ne s'imagine pas souvent les hackers être des filles sexy. Mais il y en a. De même que des filles qui travaillent dans la création de jeux informatiques, il y en a de plus en plus. Tant mieux. Un peu d'équilibre.

Vos personnages "hackers" sont très typés : Percings, tatouages... Nous sommes très loin du boutonneux seul dans son grenier. Pourquoi ?
J'ai rencontré des docteurs en sciences économiques à Oxford qui étaient des blondes sexy de haut en bas, tout comme j'ai travaillé avec des chefs de projets qui étaient des punks aux crêtes multicolores, ou encore j'ai vu un conducteur de métro habillé en Elvis Presley. Les gens sont tout autres que les stéréotypes qu'on leur attribue.

D'ailleurs, pourquoi pensez-vous que les hackers travaillent en groupe ?
Tout comme les gens qui aiment bien jouer à half-life en réseau dans la même pièce pour entendre les réactions des autres, j'ai des amis hackers qui adorent me raconter autour d'une bière ce qu'ils ont cracké pendant le week-end. C'est plus sympa à plusieurs... Si on a des amis qui aiment ça aussi :)

Vous utilisez l'informatique pour la création de vos dessins. Vous craignez les pirates ?
Non. Bon... Evidemment, dès que l'on est connecté à l'Internet, il faut s'y attendre. Je pense surtout aux modèles 3D qui, si on les vend, peuvent rapporter pas mal d'argent, mais que n'importe qui peut vous voler et utiliser. Mais je n'ai jamais entendu parler d'aucun vrai problème de piratage ou de vol de programme. Par contre, on peut toujours utiliser les services de hackers pour obtenir des programmes qu'on ne pourrait jamais se payer, et voir si ces programmes valent le coup.

Pour vous, existe-t-il une différence entre hackers et pirates ?
Pas vraiment. C'est le même genre d'activité.

Vous parlez de grands méchants de la finance ! Pensez-vous que les hackers peuvent aussi montrer les problèmes cachés dans notre société ? Dévoiler des arnaques...
Evidemment. C'est bien pour ça que l'on emploie d'anciens pirates pour en attraper d'autres. Mais pour montrer les problèmes cachés dans notre société, il faut la comprendre et savoir ce qu'on cherche. Il ne s'agit pas juste de se connecter sur l'internet et zap ! On découvre des secrets.

La police est plutôt musclée dans votre BD : gilets pare-balles, casques, armes de guerre ! Ils prennent les hackers pour des terroristes ? Vous en pensez quoi ?
Il ne faut jamais croire que le monde est sympathique. Hacker est un sérieux business, ce n'est pas une blague. On détient un pouvoir non contrôlé et la société ne tolère pas ce genre de choses.

Quel est votre pire souvenir en informatique ?
Des mois de travail perdus lors d'un crash. D'où l'adage « better save than sorry » : il vaut mieux passer 15 minutes « backing up than to be sorry ». J'ai maintenant des sauvegardes de mes fichiers en France, en Angleterre et en Allemagne. Juste au cas où il y aurait un incendie ou la guerre :)

Le meilleur ?
A chaque fois que je peux installer un programme sur un PC et que ça marche du premier coup !

Parlons un peu avenir. Que prépare Alain Maindron dans un avenir proche ?
Tout dépendra du succès de Hack & Cash. Si ça marche, je continue. Très simple. La 3D demande un travail énorme. C'est un marathon. Et en BD il faut avoir roulé pendant quelques années pour s'en sortir financièrement. Il faut donc y croire. Donc, tant que les gens achètent ce qu'on fait, on peut encore s'en sortir.

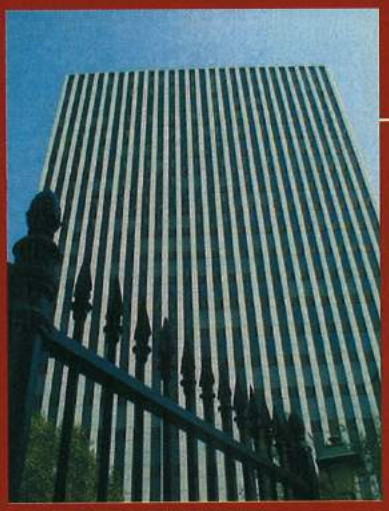
Le piratage de BD est un acte assez présent sur le web. Le fait que la vôtre le soit certainement vous gêne-t-il ?
Non. Ceux qui peuvent se payer le vrai album quand il sort, l'achètent simplement parce qu'ils aiment avoir le vrai en main. Moi, j'achète un album parce que je veux le lire tout de suite, et aussi parce que l'original est mieux qu'une copie mal photocopiée ou imprimée sur du papier journal.

L'AUTEUR

Né à Lyon en 1963, Alain Maindron a d'abord fait des études universitaires en sciences économiques, pour très vite s'apercevoir qu'il ne correspondait pas à cette orientation. Il a donc enchaîné avec l'école de BD d'Angoulême. Puis il a travaillé pour des séries TV en France, et il est parti en Angleterre pour travailler ses films et publicités. A force de bière et de fish & chips, il est devenu directeur de séquence sur le film Fro 7 avant de partir en Australie pour travailler chez Disney. Une bonne expérience professionnelle, mais Alain Maindron s'ennuyait. Il est donc revenu en Angleterre ouvrir un studio et créer des séries TV. Les ordinateurs devenant plus puissants, il s'est associé à un programmeur et tous deux ont créé un jeu ordinateur à deux, Ecstatica. Ce qui l'a amené en Californie pour travailler sur d'autres jeux et dans d'autres compagnies. Malgré une réticence au départ, il y a appris beaucoup, d'un point de vue professionnel mais aussi sur un certain état d'esprit absolument unique. Alain Maindron est revenu en France développer un studio pour créer des bandes dessinées faites par ordinateur : un moyen de création qui permet un travail collectif et une grande souplesse, notamment dans toutes les possibilités stylistiques que cela représente. La saga Les Impondérables dont Albin-Michel publie actuellement le troisième tome, est sa première série de bande dessinée.

HACK & CASH : Pour solde de tout compte

Aka, l'héroïne, fait partie d'une bande de sympathiques hackers, des marginaux passionnés d'informatique et d'infiltration du net. Aka reçoit un e-mail qui ne lui est pas destiné, et toute l'équipe de hackers s'amuse à en retrouver la piste. Résultat, ils se font tous décimer par la police, sauf Aka qui réussit à s'enfuir. Maintenant, l'unique but d'Aka, c'est de venger ses amis. Et la seule solution, infiltrer la multinationale responsable du massacre. De marginale, elle deviendra exécutive woman et retournera les armes de ses adversaires contre eux. Une nouvelle BD à l'efficacité redoutable qui n'est pas sans rappeler « Money » de Sulitzer ou « Largo Winch » de Frantz et Van Hamme.



CYBER FLIC

Depuis la fin de l'année 2002 une loi protège des pirates et autres escrocs du web, les sujets de Sa Majesté le roi des belges Albert II. Une loi et une police spécialisée dans la lutte contre la cyber délinquance, la Computer Crime Unit, que nous avons rencontrés pour vous dans les nouveaux locaux qu'ils occupent depuis quelques semaines.

Qu'est ce que la C.C.U., la Computer Crime Unit ?
C'est une des unités qui en Belgique est organisée au sein de la police fédérale pour traiter de la criminalité informatique, et pour venir appuyer la police locale et fédérale, qui sont confrontées à du matériel informatique. Notre activité est basée sur la loi dite "criminalité informatique", sur le travail d'appui et tout ce qui est lié aux demandes que peuvent nous adresser nos collègues, en rapport avec des dossier qui concernent du matériel informatique. Dans ce cas-là, nous analysons l'informatique saisie. Ils peuvent ainsi avoir rapidement des données qui peuvent être intéressantes pour leur enquête.

Etes-vous des spécialistes du piratage, hacking, virus... ?
Par la force des choses, des gens se sont spécialisés. Dans le nouveau personnel qui rejoint notre équipe, certains ont suivi des formations dans tel ou tel domaine, ou ont des expériences professionnelles. Un renfort de choix.

Vous avez un bureau dédié, Mac, PC, Linux, GSM...
Oui ! Les gens qui se chargent de ces domaines se sont spécialisés par eux-mêmes, ce sont des autodidactes. Nos nouveaux collègues, eux, sont des informaticiens de la police qui maintenant trouvent le moyen au sein de la police d'exploiter ce qu'ils ont acquis auparavant.

En Belgique, y avait-il un besoin de ce genre de section policière ?
Il y a un véritable besoin dans ce qui touche l'analyse informatique, c'est certain. On trouve de plus en plus de dossiers dans lesquels l'ordinateur est un élément déterminant dans la commission des faits, dans les problèmes financiers, par exemple. L'Internet aujourd'hui est aussi un vecteur de délit.

Dernièrement, vous avez eu de grosses affaires, vous fonctionnez comment ?
Deux tiers de notre activité correspondent à de l'appui. Le matériel nous arrive dans le cadre d'un dossier déterminé. La plupart du temps, nos actions concernent des intrusions ou le bon fonctionnement d'un serveur informatisé. Souvent du vol d'information...

Y a-t-il une prise de conscience du monde de l'entreprise ?
Oui, une prise de conscience qui commence à devenir importante. Les entreprises comprennent qu'il y a un véritable besoin de se protéger. Mais toutes les affaires qui sont liées au piratage informatique ne nous sont pas indiquées. Là où l'entreprise a pris conscience de la nécessité de sécuriser des entrepôts, des bureaux... petit à petit elle comprend aussi qu'il faut sécuriser les systèmes informatiques.

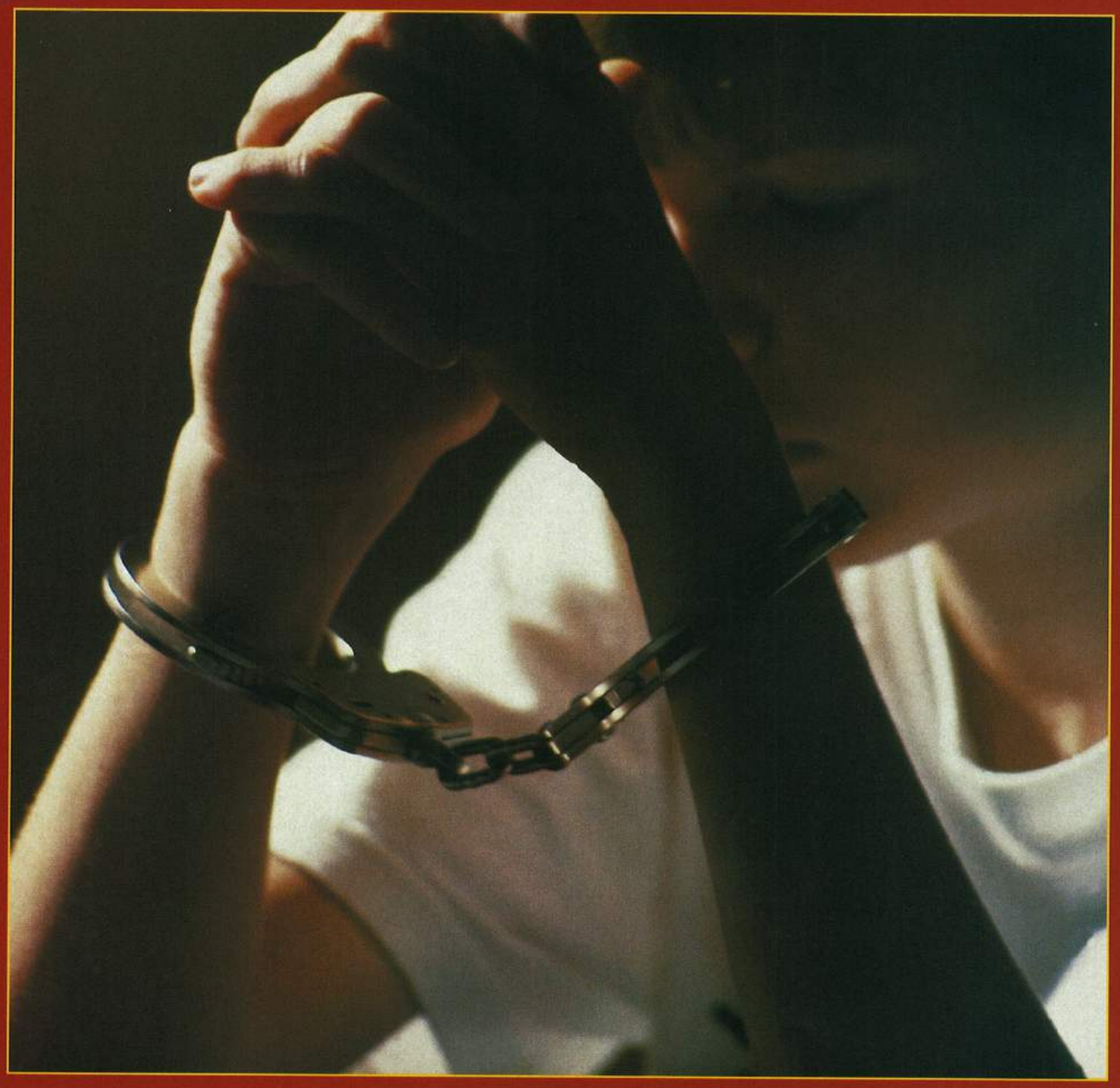
Vous avez été ceux qui avaient mis deux fois de suite la main sur le pirate Red Attack. Est-ce que ce genre d'individu remplit vos dossiers ?
Il y a beaucoup plus de dossiers qu'avant. Mais le problème est de savoir si on a plus de dossiers parce que les délits augmentent, ou parce que les victimes savent que nous sommes là, la loi et l'unité, pour les protéger et les défendre. De plus en plus de sociétés vérifient aujourd'hui les problèmes. Ce qu'ils pensaient être un plantage hier, peut en fait dévoiler un piratage après contrôle, ce qui leur permet de se défendre, de porter plainte... Donc oui, il y a une augmentation, sans qu'on puisse déterminer pour autant s'il y a un profil, ou une croissance du nombre de gens qui pratiquent ce genre de délit.

La Belgique a changé sa loi. Qu'est ce qui a changé ?
Le gros de la législation a donné des définitions précises au hacking, à la destruction de données. Elle a donné clairement une existence juridique à ce qui est immatériel. Avant, la loi faisait des assimilations. Aujourd'hui, on clarifie pleinement les choses.
On a aussi organisé les acteurs du monde informatique. Aujourd'hui les fournisseurs d'accès, les administrateurs, les internautes, ont des droits et des devoirs, leurs obligations... Le code d'instruction criminelle prévoit clairement l'obligation pour les administrateurs de fournir une assistance à la police. Il peuvent être poursuivis s'il n'aident pas à l'enquête.

N'est-elle pas un peu dure ?
Le législateur a voulu que la loi soit en phase avec une évolution technique constante. On sera contents, d'ici 5 à 6 ans, de compter sur ce texte par rapport à des évolutions de la technologie. Aujourd'hui certaines montres, par exemple, servent de supports de données. Si on ne l'avait pas su, elles n'auraient pas pu être saisies dans une affaire. Aujourd'hui la loi va les intégrer.

PIRATES BELGES, GARE À VOS FESSES UNE FOIS !

**La Computer Crime Unit est basée à Bruxelles, dans l'ancien immeuble d'IBM.
C'est au 18ème étage que nous avons rencontré l'équipe de la C.C.U. dans des locaux spacieux et plutôt impressionnants avec vue à 360 degrés sur la capitale belge.
Plusieurs pièces, toutes équipées d'informatique et de connexions intranet et internet. Chaque bureau a sa spécialité. Dans la salle des spécialistes, cachés derrière leurs machines, Ils sont les rois du MAC, de Linux, du GSM... Un autre bureau nous a impressionnés : il regorge d'ordinateurs numérotés, des dizaines de saisies qui attendent d'être contrôlées, analysées, décortiquées. La salle principale, elle, regroupe le reste de l'équipe, 14 policiers.**



Walkman mp3, montre, téléphone, n'importe quel support informatique peut ainsi être saisi.

Comment travaillez-vous avec des enquêtes visant des utilisateur du P2P ?
La problématique est double. « Droits d'auteurs », une unité spécialisée, se charge de ce cas. Pour notre unité, nous intervenons dans la localisation des gens qui mettent à disposition des centaines de logiciels, mp3, films contrefaits. Nous sommes confrontés à un vrai problème avec le Peer to Peer, surtout dans les affaires de pédophilie. Ces personnes utilisent des mots-clés bien spécifiques dans leurs échanges, et la filière est difficile à remonter. Nous avons mis en place des protocoles pour identifier.

Ca marche vraiment ?
Non ! Ce n'est pas toujours évident. C'est un vrai problème.

Et la perquisition à distance ?
La loi prend en compte cette forme de perquisition. C'est l'une des évolutions de la loi belge.

Cela fonctionne comment ?
En fait concrètement, nous recevons une ordonnance de perquisition. Lorsque l'on arrive sur les lieux du domicile du perquisitionné, que l'on constate que ses bases de données sont à l'extérieur du domicile, nous devons rédiger une ordonnance complémentaire, dans laquelle nous indiquons notre action numérique. Nous avons eu le cas dernièrement avec une banque. Les bases de données étaient hébergées en Allemagne. Le juge a étendu son mandat et notre perquisition sur cette base de données, à l'étranger. Donc nous, de la station de travail du perquisitionné à l'endroit de la perquisition, on se porte à distance dans le lieu ou nous souhaitons récupérer les données complémentaires.

De votre bureau vous pouvez agir ainsi aussi ?
Non ! Cela se fait obligatoirement sous le contrôle d'un magistrat instructeur. C'est vraiment lié à un mandat de perquisition. Cela se fait avec des règles extrêmement précises et des éléments très motivés. Ce n'est pas nous, de la C.C.U., qui allons entrer dans la machine de quelqu'un.

Un de vos souvenir les plus marquants ?
L'arrestation d'un pirate nommé Scorpio. En 12 heures de temps nous l'avions repéré et arrêté. Nous avons été aidés par les collègues de plusieurs unités,

LE SOCIAL ENGINEERING

Quel est donc ce mot étrange ? Le S.E., son autre petit nom, correspond à l'étude d'une cible afin de la pirater. Le facteur humain est l'un des maillons « faibles » de la sécurité informatique. Nous allons vous expliquer comment vous garder de ce genre de problème.

FACTEUR HUMAIN

« Le facteur humain est l'un des maillons de la sécurité informatique ». Cette phrase de Kevin Mitnick, papy du hacking, résume assez bien la situation actuelle. Les systèmes de sécurité sont de plus en plus perfectionnés, à tel point que toute personne derrière un firewall se croit à l'abri d'intrusions dans son système. Malheureusement, c'est loin d'être le cas.

Le social engineering ou encore ingénierie sociale en français, permet de contourner tous ces dispositifs, aussi stricts soient-ils. Cette méthode se base sur l'exploitation de l'abus de confiance et la volonté d'aider une personne, pour lui faire exécuter n'importe quelle action qui permettra au pirate de s'introduire sur son ordinateur. Cela peut paraître à première vue dérisoire, mais le nombre de personnes se laissant prendre au piège de « manipulateurs » est plus qu'affolant.

LES DIFFÉRENTES TECHNIQUES ET COMMENT S'EN PROTÉGER.

La méthode de social engineering la plus courante sur internet, est bien évidemment la messagerie électronique. Il faut distinguer deux buts bien distincts dans le social engineering par mail : Faire exécuter un virus à la victime et/ou récupérer ses mots de passe. Il faut tout d'abord savoir une chose : le protocole SMTP permettant d'envoyer des courriers électroniques n'est pas du tout sécurisé. Je veux dire par là que n'importe qui peut en quelques clics changer d'identité pour se faire passer pour quelqu'un à qui vous faites confiance, tel que Microsoft, Hotmail, Caramail...
Voici un exemple de mail circulant sur Internet :

```
De : Administrateur@microsoft.com
Objet : URGENT
ALERTE !!! Une faille de sécurité majeure a été découverte dans Microsoft Windows 98/Me/2000/NT/XP. Merci de télécharger immédiatement le patch de sécurité en cliquant ici.
```

Lorsque la victime va cliquer sur le lien fourni dans le mel, il y a 100 % de chances pour qu'elle se retrouve à télécharger un virus ou un cheval de Troie.

FAUX SITES

Le faux site web d'une banque australienne, ANZ, a été fermé par la police australienne et américaine début juillet. Il aura fallu près de 4 mois pour couper du web ce site monté par des escrocs qui, par mel, incitait les clients de ANZ à réactiver leurs comptes en ligne. Le même courrier a également visé des clients de la Westpac bank, avec des e-mails semblables, incitant les clients à entrer leurs informations confidentielles. Même problème pour Sony. Le géant du multimédia a été victime en juillet dernier d'une escroquerie internet par courrier électronique. Un faux mel avait été diffusé par un pirate. Il tentait de récupérer les informations privées des internautes inscrits sur le site Sonystyle.com. Sony avait encouragé ses clients à entrer en contact avec leurs banques, dans la mesure où ils avaient acheté des articles via le site Sonystyle. Un piratage de numéro de CB pouvant être possible. Le social engineering est à prendre au sérieux. Selon la société d'analyse Gartner, le vol d'identité aux Etats-Unis a augmenté de 79 % au cours de l'année dernière. Un pourcentage énorme au vu du nombre d'arrestations pour ce genre de délit, soit seulement 700 escrocs arrêtés. Sept millions d'américains ont été victimes d'un vol d'identité de juin 2002 à juin 2003.

LES VIRII SOCIAUX

Afin de se répandre aussi rapidement et aussi largement que possible, les virii ont exploité les dernières techniques d'ingénierie sociale, allant dans certains cas jusqu'à se faire passer pour des patches de sécurité de Microsoft. Par exemple, le virus Gibe (W32/Gibe) exploite des techniques toujours plus ingénieuses pour inciter les utilisateurs à exécuter des codes malveillants sur leurs ordinateurs. Gibe se propageait dans un mel ayant pour objet 'Internet Security Update' et incluant le fichier 'Q216309.exe'. Le message expliquait aux utilisateurs que le fichier attaché était un patch de sécurité de Microsoft. Totalement faux.
Les patches sont sur microsoft.com

Pour ne plus tomber dans ce vulgaire piège, deux règles d'or : ne jamais accorder sa confiance en se basant simplement sur l'adresse de l'expéditeur, il faut toujours vérifier les informations sur le site de la compagnie. Ne jamais ouvrir de pièces jointes sans les avoir contrôlées avec un antivirus mis à jour. Dans tous les cas, un logiciel se télécharge sur le site officiel de l'auteur.
Pour récupérer le mot de passe d'une victime potentielle, un pirate va encore se baser sur la confiance que l'utilisateur aura en l'émetteur. Différents messages provenant soi-disant du service client de sites de messagerie électronique, essayent d'extirper les mots de passe. Dans les grands classiques on retrouve : *« Vos informations ont été perdues pour la raison X. Merci de nous les communiquer à nouveau via le formulaire ci-joint »* *« Destruction des comptes inactifs, vous devez renvoyer ce formulaire rempli avant le xx/xx/xxxx sinon votre compte sera désactivé et tous vos messages seront détruits pour économiser de la place »*. Si vous avez déjà répondu à un tel mel, vous pouvez être sûr que vous avez donné le sourire à un pirate qui connaît maintenant votre mot de passe.
Votre fournisseur d'accès internet ou votre service de messagerie ne vous demanderont jamais vos identifiants, de même qu'aucun site de commerce électronique ne vous demandera votre numéro de carte bleue par courrier électronique. Il est donc indispensable de refuser systématiquement ces messages.
Mais un pirate déterminé ne se limitera pas au mel, et tentera de convaincre sa cible via IRC, ou autres salons de discussion en ligne. Gardez toujours à l'esprit : mettez à jour votre antivirus et faites lui confiance ! N'écoutez pas un étranger, même si il vous flatte et qu'il vous promet les rencontres les plus folles.

Allô ?
Pirate : *Bonjour Madame / Monsieur, je suis Jean Dupont de l'INSEE. Auriez-vous quelques minutes à m'accorder pour un sondage ?*
Victime : *Oui bien sûr, je vous écoute.* (Sinon le pirate n'a qu'à insister, rappeler plus tard ou changer de victime tout simplement)
Pirate : *Avez-vous des enfants ?*
Série de questions sans intérêt
Pirate : *Quels sont le nom et l'adresse de votre banque préférée ?*
La question passera sans problème au milieu de toutes les autres, le pirate continue avec d'autres questions sans intérêt et raccroche.

Nous avons des cas où le pirate va rappeler quelques jours plus tard la même personne, se faisant passer pour le responsable de la banque en question. Dans nos cas, le pirate avait pris soin de se renseigner sur le directeur de l'agence bancaire en question. Il va expliquer que la carte de la victime a été piratée et qu'il lui en faut les informations secrètes.

La solution est simple, appelez ladite banque pour avoir confirmation du piratage en question, mais ne révélez jamais votre mot de passe à quiconque vous le demanderait par téléphone.

www.soswindows.net

- Aide astuces
- Optimation Windows
- Hotligne informatique
- 100 % Gratuit

20 et 21 Septembre 2003

Ville de Liège

Congrès informatique
Liège Belgique

LE VRAI ET LE FAUX WAREZ

Depuis notre précédent article paru dans ZATAZ 6 répondant à la question posée par nos lecteurs « Y a-t-il beaucoup de boards sur l'Internet ? », nous avons reçu beaucoup de messages venus de ce milieu, ainsi que de nos lecteurs qui nous affirmaient que les boards ne sont pas issus du « vrai » warez. Vous nous connaissez, nous ne sommes pas le genre de journal qui édite des articles copiés d'internet, on aime plutôt l'enquête chez ZATAZ Magazine. Nous avons donc décidé de nous pencher sur cette affirmation et de répondre à cette nouvelle interrogation. Nous allons vous montrer les différents « groupes » du warez. De la sortie des contrefaçons sur les H.Q. jusqu'au peer to peer.

LA GENÈSE

Tout commence au moment de la sortie d'un film. Les grandes teams (Night, Centropy, TFC...) se battent pour être les premières à en réaliser la copie qui sera diffusée sur le net, via le H.Q., comprenez le quartier général du groupe. Certains n'hésitent pas à écumer toutes les avant-premières afin de filmer la nouveauté avec une caméra rudimentaire. Dès que les détails de la compression sont terminés, le film est immédiatement envoyé sur des topsites qui enregistrent la réalisation, la "releasent", et se chargent de la diffuser sur d'autres topsites (curry). Chose facilitée par des connexions utilisant des bandes passantes qui nous font tous rêver. De ce fait, en quelques heures à peine, les nouveaux films sont envoyés sur l'Internet afin d'être diffusés à travers le monde. Après leurs passages sur les topsites et H.Q., les films sont vite distribués sur des stros et parfois via des dumps pour être transférés vers d'autres lieux de diffusion. Les règles sur les H.Q. et topsites sont très sévères : Pas de classiques, pas de vieilles réalisations, pas de films mal encodés. Certains groupes interdisent certains formats de compression pour les films ou pour les mp3. Certains dupechecks refusent le rv9, le nouveau format de Real. La rumeur veut que ce format soit traçable.

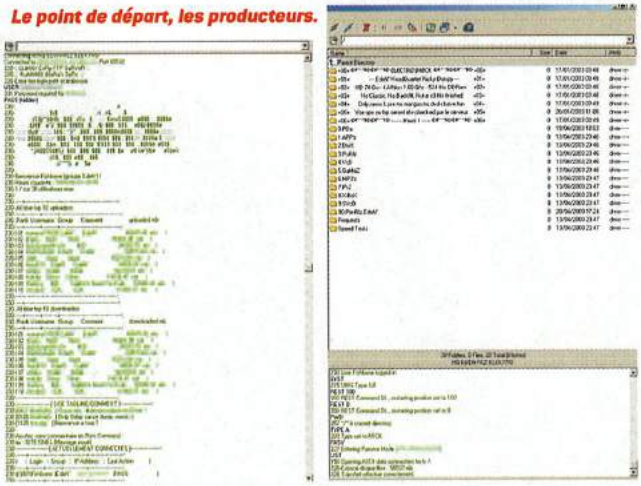
LE BON, LA BRUTE ET LES TRUANDS

Pour diffuser leurs contrefaçons, les pirates utilisent plusieurs techniques. Commençons par parler des Xdcc et Fserves. Ils constituent une assez grande partie du « warez public ». Les Xdcc et Fserves sont bien souvent faits à l'aide d'ordinateurs piratés via des failles qu'utilisent aussi les defacers, les barbouilleurs de sites web, ou encore les pédophiles. Les failles les plus communes étant IPC nullsession, SQL nullsession, Webdav, IIS... Ce sont des bots, des robots IRC qui gèrent un espace défini sur les ordinateurs piratés sur le réseau. Ces bots font le lien entre la machine piratée et le « pirate ». Cela va lui permettre de télécharger sans contrainte.

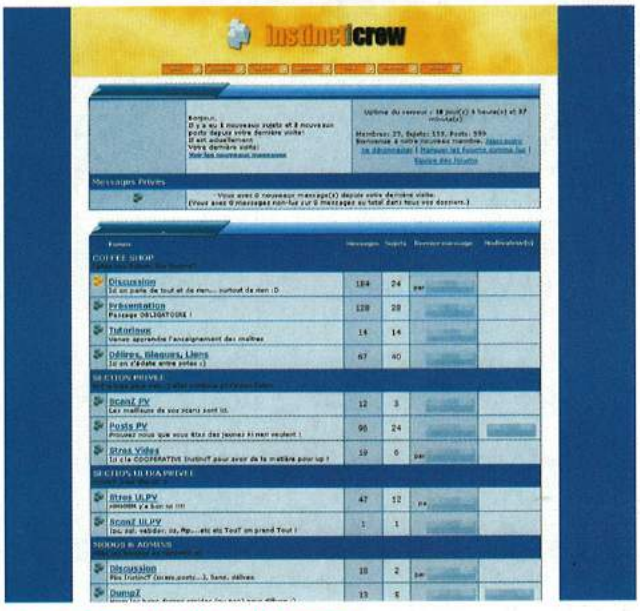
ON RIGOLE PAS AVEC LES RÈGLES

Les groupes qui diffusent films, logiciels, mp3, via un ring, ne rigolent pas avec les règles. Il en va de « l'honneur » du groupe. Voici quelques règles auxquelles sont tenus les membres. Si ces derniers ne les respectent pas, ils se retrouvent avec des « points » en moins dans la hiérarchie du groupe, voire exclus complètement sans autre forme de procès. Un film qui ne sera pas uploadé, téléchargé vers le ftp du groupe, dans un bon dossier, vaudra par exemple 3 points de moins à l'auteur de « l'erreur ». Un Nuke x3. Si un membre du chan a le malheur de parler du ring ou du chan groupe sans demander l'autorisation à un admin, il passe en mode DEL USER ; comprenez : il prend la porte et son accès est annulé.
Certains groupes n'hésitent pas à mettre en place de véritables feuilles d'évaluation mensuelle, permettant ainsi de gratifier les meilleurs éléments d'accès plus importants, et de mettre à l'index les plus « feignants ». Ces feuilles, que nous avons pu trouver sur internet avec Google, montrent par exemple le nombre de membres de telle à telle date. Le nombre de «stros fournis», le nombre de ranges scannées, et les failles par membre scanneur. le nombre de Divx, par exemple, réalisés...

Le point de départ, les producteurs.



Ensuite, dans la même catégorie, nous allons trouver les boards. Nous vous en avions parlé amplement dans le ZATAZ magazine 6 et 7. Les boards sont des lieux de regroupements de pirates, de releasers, de diffuseurs, de graphistes et de plein d'autres talents perdus. Des lieux où le warez fait rage à travers stro, ftp anonyme, et parfois dump ou dump team. Des lieux de stockage de releases faites par certaines boards et distribuées sur le réseau des réseaux. Toutes les releases des boards sont enregistrées sur des dupechecks. Les dupechecks sont des endroits où les teams peuvent vérifier les films déjà releasés pour ne pas les enregistrer une seconde fois, dans le même format de compression par exemple.
Ne nous voilons pas la face. Certains importants groupes warez ont des



Les rlz finissent ensuite sur les boards E.

10922, 10923, 10924. A 11 000 j'arrête !

membres qui ont des contacts dans le milieu du film et du disque, de la presse ou des attachés de presse. Des contacts, voire un métier, qui permet d'avoir accès aux DVD avant leur apparition dans les magasins. C'est d'ailleurs pour cela que de plus en plus de «preview press» sont protégées contre certains journalistes un peu trop légers avec ce qui leur a été envoyé. Tous ces «pirates» expliquent ne pas vouloir se faire connaître, ni citer. Nous l'avons vu pendant notre enquête qui aura duré, mis bout à bout, 4 mois. Pourtant ils veulent tous être les premiers à sortir LE film, pour que leurs pseudos soient connus à travers le net. On ne connaît pas de groupe qui réalise des copies pour qu'elles ne soient pas diffusées. Les règles du warez sont claires. Il faut le nom du groupe et un fichier attaché au film, nommé nfo. Des fichiers qui permettent souvent d'avoir des tonnes d'informations sur ces teams. Discrets mais pas trop !

BACK TO THE FUTUR

Le warez c'est aussi de vieux trucs, un peu désuets ou moins connus, qui servent à la diffusion ou les échanges. Commençons par Bobdown. Ce programme permet de télécharger des fichiers stockés sur un serveur FTP ou HTTP tout en évitant le besoin d'avoir un client FTP. Il permet aussi de cacher à la vue du downloader l'adresse IP du serveur ftp. Cela permet aux groupes d'éviter les jalousies qui finissent toujours par l'effacement des fichiers ou le piratage du « stros » par un groupe concurrent.

Viennent ensuite les FTP à ratio. Beaucoup de FTP permettent un téléchargement illimité mais certaines organisations, surtout de leech, utilisent les ratios de téléchargement sur les FTP pour encourager les utilisateurs à partager avec les autres, les nouveautés warez. Certaines grandes teams, ou rings, utilisent aussi les ratios pour contrôler les diffusions de leurs réalisations. Cela permet aussi de contrôler ce qu'apportent les membres sur le ftp. Les rings sont des rassemblements de teams sur un canal IRC où se trouvent des bots qui annoncent en temps réel les nouvelles productions pirates. Des copies qui peuvent être téléchargées sur des HQ ou Dumps. Il paraît que cela permet une meilleure gestion des espaces de diffusion et un meilleur contrôle des utilisateurs. En gros, d'éviter de voir les copies se faire télécharger par des gens qui n'apportent rien. Parlons ensuite des newsgroups. Ils sont aussi appelés

Les groupes warez affichent leurs dernières releases.

WAREZ FRANÇAIS DANS LA LIGNE DE MIRE

Des ordinateurs de l'état du Kentucky ont servi de lieux de stockage pour des copies pirates de films et logiciels. Voilà ce que viennent d'annoncer des investigateurs du F.B.I. Les agents pensent que les intrus sont des français et des canadiens, qui ont utilisé ces ordinateurs pour stocker des fichiers électroniques piratés, comme des films et des jeux vidéo. Le système a été corrompu le 2 avril dernier et largement employé ensuite. Les agents du F.B.I. enquêtent pour savoir si les pirates, qui ont eu accès à l'interface de gestion, ont pu aussi modifier des dossiers et documents qui se trouvaient sur le réseau. Les adresses des pirates sont basées en France, au Canada et en Croatie. Le serveur hébergeait le dernier Tomb Raider, ainsi que Spy Kid 3D ou encore des livres médicaux. Bref, un stro et des stro« teurs » dans la besace de l'Oncle Sam.

« Forum Usenet ». Les newsgroups servent de lieu de diffusion de programmes warez en fichiers binaires.

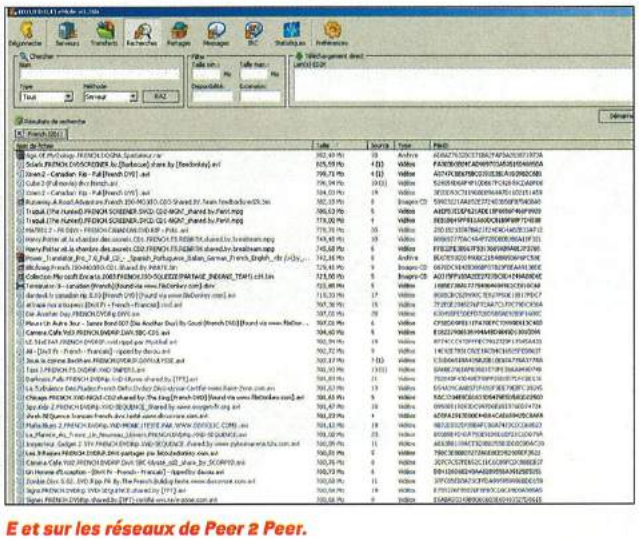
Beaucoup d'internautes, depuis un certain moment maintenant, utilisent des systèmes peer to peer. Les logiciels de P2P sont les lieux sur le réseau où tous les jours des millions de copies d'albums de musique, de films, de logiciels, sont diffusés. Edonkey, E-mule, Kazaa, Bit Torrent, Shareaza, Gnutella, Limeware, en sont quelques exemples. Le principe est très simple. Des liaisons entres les PC des clients permettent l'échange décentralisé de l'information à travers le Net. Malheureusement, le but primaire des réseaux peer to peer à la base, était de permettre une meilleure diffusion de l'informatique sur le Web. Il faut croire que tout ce qui peut faire du bien peut aussi très bien faire beaucoup de mal.

Les hotlines sont un peu comme les réseaux p2p. Ils se différencient par le fait qu'ils sont des programmes client/serveur, la plupart du temps privés, contrairement à la forme client/client, public, des réseaux p2p. Un canal de chat permet de discuter avec les autres membres connectés sur le serveur. Les fichiers copiés y sont conservés pour les usagers ayant accès à la hotline.

Bien sûr, il restera toujours les moyens physiques d'échange de copies pirates. Des organisations mondiales qui se font de l'argent sur le dos des compagnies commerciales de jeux, de films et de musiques, ou de l'un de vos «potes» qui vend le dernier film à la mode téléchargé via... le peer to peer.

PIRACY IS MY LIFE, MY LIFE IS MY BUSINESS

Il est impossible de tout déceler. N'importe qui dans son salon peut copier un CD ou un DVD et le revendre. La consommation de loisirs à outrance, la démocratisation de l'informatique, ont tué le warez, le vrai. Celui qui n'avait qu'un seul but, permettre le test d'un logiciel avant de l'acheter. Il reste encore quelques «purs», ils sont cachés dans les HQ, les rings, voire certaines boards. Mais jusqu'à quand ? La justice, les majors, et la bêtise d'un trop grand nombre d'utilisateurs va tuer l'essence même de l'éthique warez.



E et sur les réseaux de Peer 2 Peer.

TOUT SUR LA CRYPTOGRAPHIE

Qu'est-ce que la crypto ? Beaucoup se perdent et se mélangent entre les termes de cryptographie, décryptement, chiffrement, cryptanalyse... La cryptographie en informatique est utilisée dans le cadre de la sécurité. Elle se base surtout sur des problèmes mathématiques très complexes, permettant ainsi de garantir la confidentialité de l'information, l'intégrité des données, l'authentification de l'expéditeur. Ce dossier spécial crypto aura pour but de vous donner une vue d'ensemble des techniques utilisées actuellement en informatique.

GARANTIR LA CONFIDENTIALITÉ

Afin de garantir la confidentialité, le texte voulu est passé dans un algorithme qui va le transformer en un cryptogramme. Actuellement, il existe deux types d'algorithmes de chiffrement ayant chacun des avantages et des inconvénients. Les plus anciens sont les algorithmes dits symétriques, ou à clef secrète. Ils sont plus simples et plus rapides. C'est grâce à ces propriétés qu'ils sont utilisés pour chiffrer les données. Les seconds, plus récents, sont dits algorithmes asymétriques, ou à clef publique. Ils sont beaucoup plus efficaces que les premiers, mais aussi beaucoup plus lents. Ils sont donc souvent utilisés pour échanger une clef secrète qui servira tout le long de la session (cf. Partie 3 : Authentification mutuelle) et pour signer les données comme nous le verrons plus loin. Ci-dessous, une description plus détaillée du fonctionnement de ces deux catégories d'algorithmes.

ALGORITHME SYMÉTRIQUE

Cette classe d'algorithmes repose sur des propriétés mathématiques très fortes. On les dit symétriques, car c'est la même clé qui code et qui décode les données. Par exemple, Adeline et Bertrand désirent s'échanger des messages mais ne veulent pas qu'un tiers puisse les lire. Ils se mettent donc d'accord sur une clé commune dite « clé secrète ». Cette clé doit rester connue d'eux seuls s'ils ne veulent pas de fuites.

Le principe de ces algorithmes est très simple : Adeline encode son message grâce à la clé secrète puis envoie le cryptogramme à Bertrand. Celui-ci, connaissant la clé secrète, décode donc le message en provenance d'Adeline. (cf. Figure 1)

Il existe deux méthodes de chiffrement : continue ou par blocs. La première agit sur un bit à la fois. L'algorithme le plus usité de ce type est le RC4 à clé variable (en général, les clés sont de 128 bits).

Les algorithmes par blocs, quant à eux, agissent non pas bit-à-bit, mais par blocs de données qui ont généralement une taille de 64 bits. Par exemple, l'algorithme DES qui utilise des clés de 56 bits, chiffre chaque bloc un à un puis les envoie dans l'ordre. L'algorithme le plus utilisé dans cette catégorie de clé est le 3DES qui est en fait une répétition d'un DES trois fois de suite avec trois clés distinctes, ou d'une suite chiffrement-déchiffrement-chiffrement avec deux clés distinctes. On trouve également souvent des algorithmes par blocs avec des clés de 128 bits comme IDEA et CAST-128 ou de tailles variables comme l'AES de Rijndeal qui chiffre avec des clés de 128, 192 ou 256 bits et le Blowfish dont les clés peuvent atteindre 448 bits !

ALGORITHME ASYMÉTRIQUE

Ces algorithmes plus récents ont été introduits en 1976 par Diffie et Hellman. Ils sont très proches des algorithmes à clé secrète. Leur seule différence est, comme leur nom l'indique, l'asymétrie entre le codage et le décodage. Cette propriété vient du fait que la clé de chiffrement n'est pas la même que celle qui sert au déchiffrement. On en garde une secrète, que l'on appellera « clé privée », et on en diffuse une, qui sera nommée « clé publique ». Le fait qu'avec nos connaissances mathématiques actuelles et la puissance de nos machines, il soit presque impossible de déduire une clé de l'autre, rend ces algorithmes très efficaces. En diffusant la clé publique, on peut en faire deux utilisations différentes : soit un tiers chiffre avec la clé publique des données qui ne pourront donc être lues que par le possesseur de la clé secrète, ce qui certifie la confidentialité des informations, soit le possesseur de la clé chiffre ses informations avec sa clé secrète, ce qui permet de vérifier leurs origines. Il existe de nombreux algorithmes sachant faire soit l'un ou soit l'autre, mais seulement trois permettent de faire les deux de façon transparente : ElGamal, RSA et Rabin.

Le principe est très simple (cf Figure 2) tant pour assurer la confidentialité (Adeline chiffre avec la clé publique de Bertrand qui peut déchiffrer le message avec sa clé privée) que pour signer numériquement le message. Ces algorithmes ont été introduits pour éviter que des tiers puissent intercepter la clé secrète lors de l'échange, et puissent se faire passer pour l'une des deux parties. Mais il ne faut pas confondre la longueur des clés secrètes avec celle

Figure 1

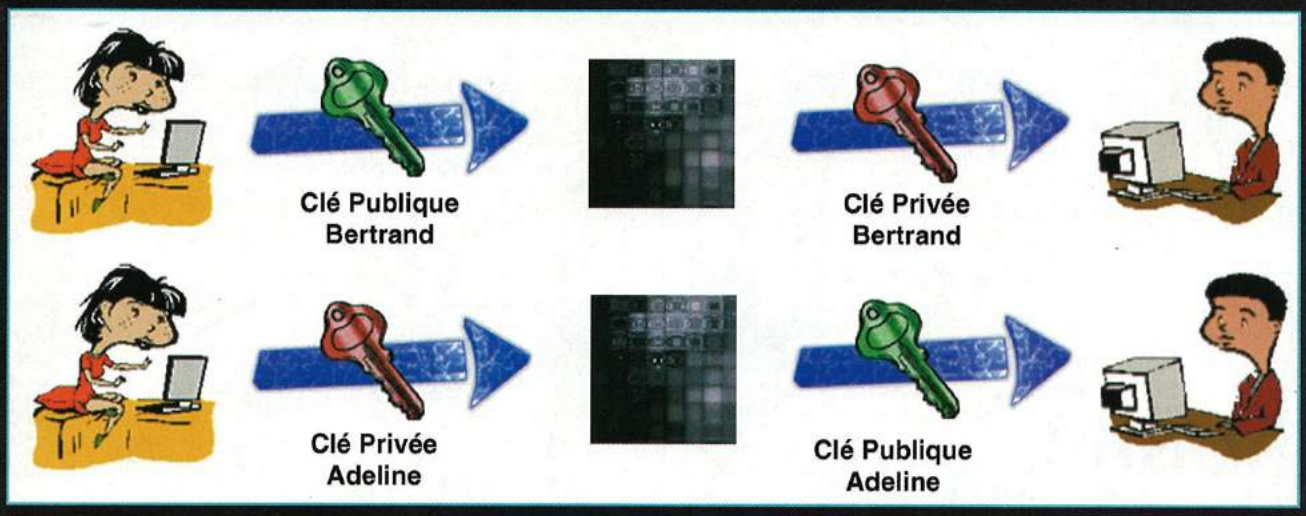


Figure 2

des clés publiques. Ces dernières, souvent très longues, dépendent uniquement de l'algorithme utilisé. De plus, nous devons être sûrs que les données qui nous parviennent sont bien celles que nous attendons. C'est l'objet de la seconde partie.

CERTIFIER L'AUTHENTICITÉ DES INFORMATIONS

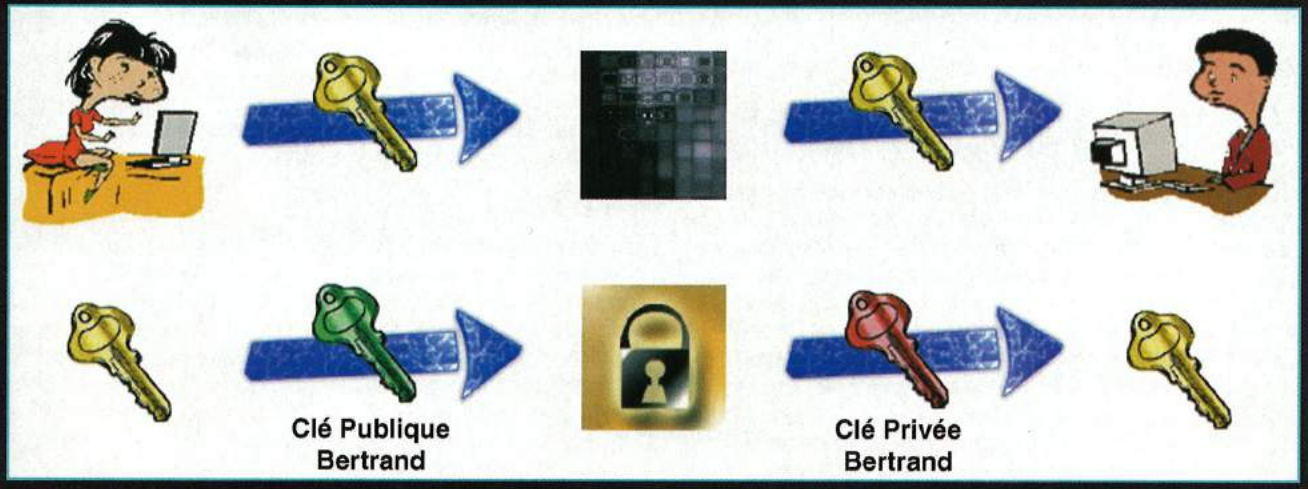
Les besoins de l'informatique ne s'arrêtent pas à la confidentialité de l'information. Les protagonistes des échanges ont besoin d'être assurés que l'information qui leur arrive est bien celle qui a été envoyée, et que la personne avec laquelle ils communiquent est bien celle qu'elle prétend être.
Les problèmes soulevés par ces questions sont l'intégrité de l'information et l'authentification des données. Ces deux notions sont inséparables en terme de cryptologie d'informatique. Elles sont regroupées sous le terme d'authenticité de l'information. D'ailleurs, on utilise souvent le mot authentification en pensant en réalité à l'authenticité.
Plusieurs méthodes rendent possible la communication avec un tiers en s'assurant qu'il est bien la personne voulue, et que ces messages ne sont pas modifiés. Par exemple, si l'on dispose d'un canal sûr mais lent et d'un autre beaucoup moins sûr mais très rapide, on envoie le message sur le canal rapide et uniquement une empreinte du message sur le canal certifié.
Ceci permet d'allier intégrité et efficacité. Dans le cas – qui est le plus courant d'ailleurs – où l'on ne dispose pas de canal sûr, comment certifier l'authenticité de l'information ? Un tiers peut recalculer l'empreinte du message qu'il a modifié. On doit donc trouver un moyen de s'assurer que seul l'émetteur peut calculer l'empreinte. C'est le rôle de l'authentification.

De même, si l'on authentifie les données sans en vérifier l'intégrité, un tiers peut modifier l'information et donc faire croire au destinataire que c'est l'émetteur authentifié qui la lui envoie.

FONCTION DE HACHAGE

L'intégrité est donc indispensable. Pour cela, on utilise une fonction de hachage, dite aussi « de condensation ». Elle prend en entrée une chaîne de longueur quelconque, et rend une nouvelle chaîne de taille inférieure (généralement fixe). Cette dernière est appelée une empreinte, ou un condensé (digest en anglais). Mais ces fonctions peuvent être faciles à inverser, ce qui ne les rend que peu sûres. En réalité, on demande à ces fonctions d'être à sens unique. Les fonctions à sens unique sont des fonctions qui sont faciles à calculer, mais très difficiles à inverser. Ceci empêche un adversaire qui n'a pas la clé de hachage de transmettre des informations erronées au destinataire.
Les fonctions de hachage à sens unique les plus connues sont le MD5 qui est ancien mais toujours utilisé, et le SHA. Ce dernier existe en deux versions : SHA-1 datant de 1994 qui renvoie des empreintes de 160 bits et SHA-2 qui permet d'obtenir des empreintes de plus grande taille. C'est d'ailleurs cet algorithme de 2000 qui est la norme NIST (National Institute of Standards and Technology) actuelle. Avec moins de quelques centaines de bits, les fonctions de hachage pourraient rendre des empreintes identiques pour deux données différentes. On demande donc aux fonctions de hachage d'être sans collision. Cette propriété, mathématiquement accessible car la quantité de chaînes est dénombrable (c'est-à-dire que l'on peut la représenter par un

Figure 3



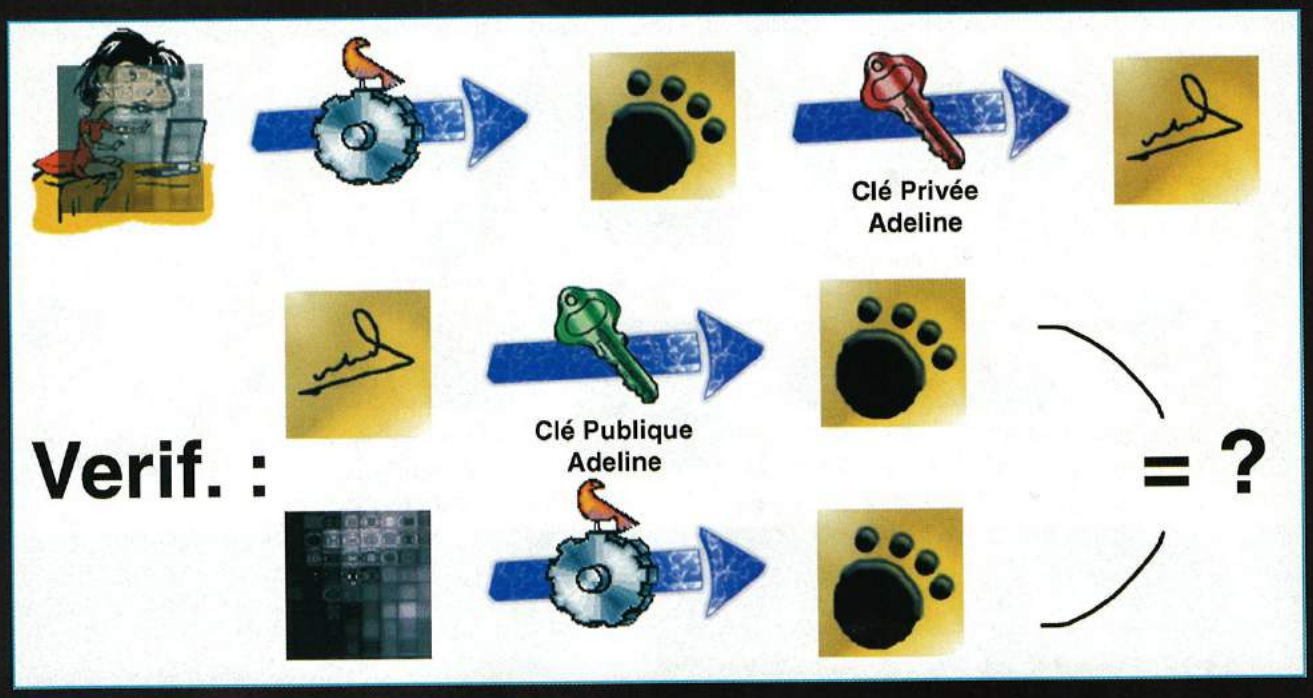


Figure 4

nombre entier), est respectée dans les deux exemples ci-dessus mais pas pour toutes les fonctions de hachage.

SIGNATURE

La signature numérique permet de vérifier l'authenticité du message. Elle se base sur les algorithmes de chiffrement à clé publique. En chiffrant le message avec sa clé privée, on assure au destinataire l'origine de celui-ci, et le résultat du déchiffrement avec la clé publique permet de vérifier l'intégrité et la non-répudiation du message. Le problème redondant de la lenteur de ces algorithmes asymétriques rend cette méthode peu utilisée actuellement. La signature est malgré tout basée sur ce principe. Grâce aux fonctions de hachage, on peut améliorer grandement l'efficacité de cette méthode. Comme le montre la figure 4, Adeline crée sa signature numérique en passant son message via la fonction de hachage, puis en chiffrant l'empreinte à l'aide de sa clé publique. Le condensé étant de très petite taille par rapport au message lui-même, le chiffrement est très rapide.
Pour vérifier l'authenticité du message, Bertrand n'a plus qu'à déchiffrer la signature d'Adeline avec la clé publique de celle-ci pour obtenir l'empreinte précédemment calculée, et passer son message reçu via la fonction de hachage choisie par Adeline. La comparaison des deux empreintes valide l'intégrité et l'authentification de l'information, tout en entraînant la non-répudiation du message. Les algorithmes de signature sont donc la somme d'une fonction de hachage et d'un algorithme de chiffrement. Le plus utilisé est le RSA qui correspond au MD5 ou SHA-1 accompagné du RSA, même si la norme NIST est le DSS (SHA-1 + ElGamal.)

SCELLEMENT

Le scellement permet de vérifier l'authenticité d'un message mais sans la propriété de non-répudiation, car un sceau est calculé à partir d'un algorithme à clé secrète. Le message est passé à travers une fonction de hachage à sens unique dépendant d'une clé secrète, ou une fonction de chiffrement par blocs. Le résultat est appelé « Code d'Authentification du Message » (MAC) ou plus communément « sceau ». En fonction de la méthode utilisée, le sceau ne sera pas le même : si l'on utilise un algorithme de chiffrement symétrique en CBC, le MAC correspond au dernier bloc du cryptogramme, si l'on utilise une fonction de hachage dépendant d'une clé secrète, ce que l'on donne à calculer diffère car l'empreinte est déjà de taille réduite. Pour la méthode de Keyed-MAC, on passe via la fonction de hachage soit la concaténation du secret et du message (dit préfixe secret), soit la concaténation du message et du secret (dit suffixe secret), soit la concaténation du secret, du message et encore du secret (dit à enveloppe secrète). Mais cette méthode datant de 1992 est à sécurité limitée. On préférera utiliser maintenant l'algorithme HMAC qui est plus subtil : on tronque le message avant de le hacher, en ne conservant généralement que le début et la fin du message à hacher.

AUTHENTIFICATION MUTUELLE AVEC ÉCHANGE DE CLÉS

Régulièrement, la cryptologie a besoin d'accomplir une série d'étapes dans un langage commun permettant à plusieurs participants d'accomplir une tâche. C'est ce que l'on appelle un protocole, comme par exemple en télécommunications. L'authentification mutuelle avec échange de clés est un protocole cryptographique. La « tâche » à accomplir pour ce protocole, est de rendre confiants les tiers qui ne le sont pas au début de la communication, et donc de supprimer l'espionnage et la tricherie.

Comme le stipulait la première partie, les algorithmes symétriques sont beaucoup plus rapides que les algorithmes asymétriques. Ces derniers sont beaucoup moins facilement décryptables par des tiers. La faiblesse des algorithmes à clé secrète réside dans l'échange des clés elles-mêmes. Cet échange doit être sécurisé afin d'éviter à quiconque d'intercepter la clé secrète, et donc de déchiffrer les informations.
Le protocole décrit ci-dessous permet d'échanger, grâce aux algorithmes à clé publique, une clé dite de session qui servira au chiffrement des algorithmes à clé secrète. L'utilisation de la première catégorie d'algorithmes assure l'authentification mutuelle des participants, et l'utilisation de la clé de session étend cette authentification à toute la durée de la connexion.
Il existe deux protocoles d'authentification mutuelle avec échange de clés : le transport et la génération.

TRANSPORT

Le transport RSA est le protocole utilisé dans SSL pour l'échange de clés de session. Il est très simple mais implique une contrainte : l'un des deux participants doit connaître la clé publique de l'autre. Un algorithme asymétrique est utilisé pour chiffrer la clé de session. Adeline possède la clé publique de Bertrand. Elle génère aléatoirement une clé secrète, puis la chiffre avec la clé publique de Bertrand. Ce dernier étant le seul à pouvoir la déchiffrer grâce à sa clé secrète, est assuré que personne n'a pu intercepter la clé de session. Ainsi, les deux participants peuvent donc chiffrer leurs informations avec cette clé grâce à un algorithme symétrique.

GÉNÉRATION

Cette méthode, introduite par Diffie et Hellman en 1976, permet de générer un secret partagé sans avoir d'information préalable sur l'autre participant. Cet algorithme permet de supprimer une contrainte non négligeable par rapport au transport. Concernant la cryptanalyse, l'algorithme utilisé est basé sur la cryptographie à clé publique qui ne dépend que de la difficulté à calculer des logarithmes discrets sur un corps fini (Z/nZ).

L'enchaînement de tâches de ce protocole est représenté sur la figure 5.
Le principe est le suivant :
- Adeline et Bertrand se mettent d'accord sur un grand entier n tel que (n-1)/2 soit premier (divisible par 1 et par lui-même uniquement) et sur un entier g primitif avec n. (Leur plus grand diviseur commun est 1). Ils se concertent de façon publique, la connaissance de ces chiffres n'étant d'aucune utilité future à un adversaire.
- Adeline de son côté, choisit un grand nombre entier a qu'elle garde secret. Elle calcule : A = g a mod(n). Bertrand fait de même en générant b puis en calculant B = g b mod(n).
- Adeline et Bertrand s'échangent ensuite, toujours de façon publique A et B.
- Adeline peut ainsi calculer : CAB = B a mod(n) et Bertrand, CBA = A b mod(n).

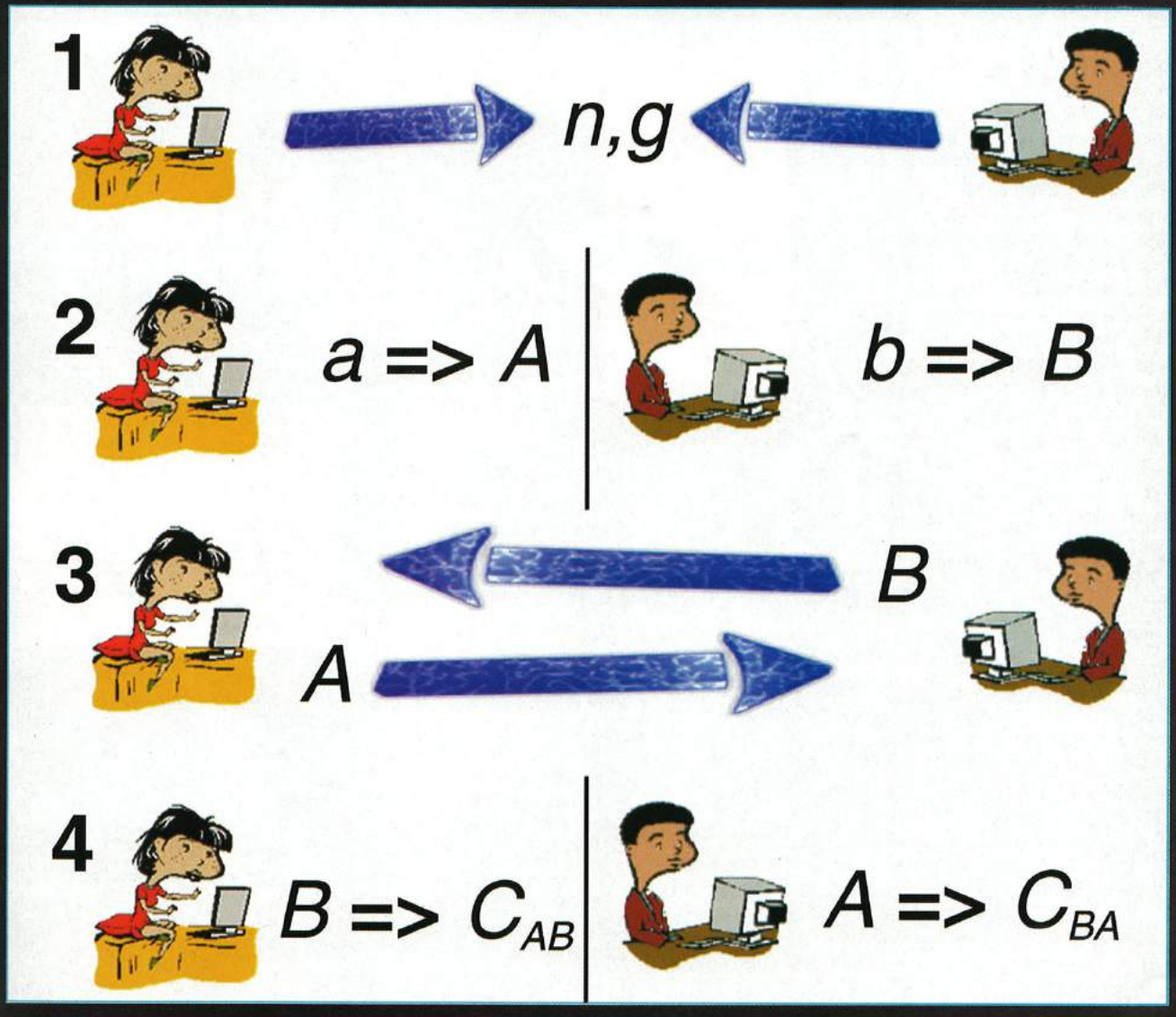
Or, comme CAB = CBA = g ab mod(n), ils possèdent à présent un secret partagé. De plus, celui-ci, avec nos capacités de calcul actuelles, ne peut être recouvré par un tiers à partir de g, n, A et B. Il existe tout de même une limitation à ce protocole. Si un intercepteur envoie sa valeur publique à la place d'Adeline et de Bertrand, il partagera un secret commun avec les deux. Ce qui lui permet de déchiffrer les messages qu'il interceptera par la suite. Afin de résoudre ce problème, il faut authentifier les valeurs publiques grâce aux certificats (comme dans SKIP) ou en signant les valeurs publiques échangées (comme dans Photuris ou IKE). C'est ce que l'on appelle le protocole DH Authentifié. On retrouve alors la contrainte du transport : il faut que chacun des participants ait une information sur l'autre avant le début de la session.

PFS (PERFECT FORWARD SECRECY)

Le protocole DH Authentifié reste tout de même nettement meilleur que le transport, car il conserve toujours sa propriété de PFS. Celle-ci empêche un adversaire qui découvre un secret à long terme, de compromettre les clefs de sessions générées précédemment. Le PFS assure plus précisément que les clés de session ne pourront pas être retrouvées à partir des secrets à long terme, et que la découverte d'une clé de session ne compromet pas les autres sessions, ni les secrets à long terme.
Ainsi, dans le DH Authentifié, comme les secrets à long terme sont utilisés uniquement pour l'authentification, et que les secrets à court terme sont les valeurs publiques du protocole DH, on a bien la propriété de PFS.

P.S. : *Vous retrouverez une série de logiciels de cryptographie et de chiffrement sur ZATAZ Magazine Online – zataz.com – via l'espace réservé aux lecteurs de ZATAZ.*

Figure 5



LES BUFFERS OVERFLOW

Faille de buffer overflow, vulnérabilité due à un dépassement de tampon, fonction strcpy() peu sécurisée... Ces termes reviennent de plus en plus dans les actualités de la sécurité informatique. Les utilisateurs, de plus en plus informés, appliquent les mises à jour ou les correctifs, mais rares sont les personnes qui comprennent vraiment l'origine de la faille. Zataz a donc décidé de sortir un peu de ses habitudes pour vous proposer cet article plus orienté technique, expliquant la source même de la vulnérabilité.

BUFFER OVERFLOW, KÉSAKO ?

Avant de commencer, il est nécessaire de rappeler un peu le fonctionnement d'un programme lorsqu'il est lancé par votre ordinateur.
Le programme va se charger dans la mémoire de votre ordinateur et définir 3 zones :
La zone texte qui contiendra le programme lui-même.
La zone données qui contient par exemple les variables statiques auxquelles le programme a besoin d'accéder.
La pile qui permet de sauvegarder des données (après un calcul par exemple) pour les transmettre d'une partie du programme à l'autre.

C'est aujourd'hui à la pile que nous allons nous intéresser. Lorsqu'un programme transmet des informations à une fonction grâce à la pile, il va placer le pointeur EBP à l'endroit où commence la partie de la pile qui va intéresser la fonction. La mémoire de votre ordinateur ressemble donc pour l'instant à l'image 1.

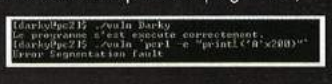
Le programme va maintenant poser sur la pile différentes choses :
Le pointeur EIP qui contient l'adresse où s'est arrêté le programme pour qu'il puisse reprendre ensuite au même endroit.
Une sauvegarde de EBP.
Et enfin les données, la pile ressemblera donc à l'image 2.

Voici ce que cela donne dans la pratique.
Imaginons le petit programme suivant que l'on appellera « vuln ».

```
/*********************************************/
main (int argc, char **argv)
{
char donnees[100] ;
strcpy (buffer, argv[1]) ;
}
/*********************************************/
```

ANALYSE RAPIDE DU PROGRAMME :

On définit un espace « données » de 100 caractères. On copie le premier argument de la ligne de commande dans cet espace. (L'argument de la ligne de commande est ce qui suit le nom du programme quand vous le lancez par MSDOS ou dans un Shell linux, par exemple si je lance « administration.exe Darky » alors « Darky » est le 1er argument de la ligne de commande. Cela peut par exemple indiquer au programme qu'il va se connecter sur le compte de cet utilisateur, ndlr). Ce fameux argument se retrouve donc dans l'espace « données » de la pile au dessus de EBP et EIP. Si jamais on envoie plus de 100 caractères au programme, que va-t-il se passer ? Eh bien, ça va déborder tout simplement, et les données vont se retrouver dans l'espace réservé à EBP et à EIP ! Cela aura pour premier effet de faire planter le programme, démonstration avec notre image 3.



Petite précision : `Perl -e « print ('A' x 200) »` envoie 200 fois la lettre A comme premier argument, ça évite de taper les 200 lettres à la main. La théorie est donc confirmée. Notez que vous obtiendrez le même résultat sous Windows. La question que vous devez vous poser maintenant est « Mais que deviennent EBP et EIP dans l'histoire, vu qu'on a pris leur place ? » Nous allons y répondre grâce à un débogueur, j'utiliserai le fameux gdb.
On lance gdb sur notre programme : `[darky@pc2]$ gdb -q vuln`
On est maintenant dans gdb et on lui demande d'exécuter le programme grâce à la commande « run » toujours en ajoutant les 200 A grâce a la commande Perl :

```
(gdb) run `Perl -e « print ('A' x 200)`
Starting program:
/home/darky/zataz/bufferoverflow/vuln `Perl -e
« print ('A' x 200)`
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
```

Notre erreur revient comme prévu, on demande maintenant EBP et EIP.

```
(gdb)info reg ebp EIP
ebp 0x41414141  0x41414141
eip 0x41414141  0x41414141
```

Vous remarquez qu'il ne contient que des 41. En fait le nombre 41 est le code ASCII de la lettre A. On a donc réussi à écrire dans EIP, alors il doit être possible d'y inscrire la valeur que l'on veut ; or si vous avez suivi la théorie du début, vous savez que EIP contient l'adresse à laquelle le programme va continuer. Vous comprenez maintenant comment des pirates détournent un programme pour lui faire exécuter ce qu'il veut en travaillant via la zone de données. Dernier obstacle : il faut trouver l'adresse de cette zone « données ». Pour cela nous allons désassembler la fonction main() du programme grâce à gdb, voir image 4. Vous n'y comprenez rien ? Pas de panique, c'est normal : il faut simplement repérer à quel moment le programme fait appel à la fonction strcpy() puisque le problème est là. Toutes les informations nécessaires se trouvent sur cette ligne : `call 0x8048300 <strcpy>`

```
(gdb) disass main
Dump of assembler code for function main:
0x80483f0 <main>:       push %ebp
0x80483f1 <main+1>:     mov %esp,%ebp
0x80483f3 <main+3>:     sub $0x78,%esp
0x80483f6 <main+6>:     cmpl $0x1,0x8(%ebp)
0x80483fa <main+10>:    jle 0x8048414 <main+36>
0x80483fc <main+12>:    add $0xfffffff8,%esp
0x80483ff <main+15>:    mov 0xc(%ebp),%eax
0x8048402 <main+18>:    add $0x4,%eax
0x8048405 <main+21>:    mov (%eax),%edx
0x8048407 <main+23>:    push %edx
0x8048408 <main+24>:    lea 0xffffff9c(%ebp),%eax
0x804840b <main+27>:    push %eax
0x804840c <main+28>:    call 0x8048300 <strcpy>
0x8048411 <main+33>:    add $0x10,%esp
0x8048414 <main+36>:    xor %eax,%eax
0x8048416 <main+38>:    jmp 0x8048418 <main+40>
0x8048418 <main+40>:    leave
0x8048419 <main+41>:    ret
End of assembler dump.
```

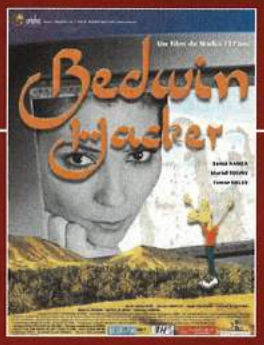
On va définir un breakpoint, un arrêt du programme, à cette adresse :

```
(gdb) b *0x804840c
Breakpoint 1 at 0x804840c: file vuln.c, line 4.
```

Il ne reste plus qu'à relancer le programme et on demande maintenant à gdb de nous donner l'adresse des données :

```
(gdb) print &donnees
$1 = (char (*)[100]) 0xbffff998
```

On sait maintenant que les données se trouvent à l'adresse 0xbffff998. Il suffit maintenant de remplacer l'adresse de EIP par celle-ci, et toutes les instructions contenues dans la zone « données » seront exécutées !
Vous savez maintenant à quoi sert l'installation de patches qui corrigent les failles de buffer overflow. Dans le prochain numéro, nous protègerons vos propres programmes contre ce type de vulnérabilité.



BEDWIN HACKER

La réalisatrice Nadia El Fani a sorti le 16 juillet un film sur l'hacktivisme. Une histoire pas comme les autres, vue par un regard autre que celui d'Hollywood. Rencontre exclusive pour ZATAZ Magazine.

Vous avez sorti en salle le 16 juillet Bedwin hacker, pourquoi un tel sujet ?

Ce qui me plaît dans le hacking c'est la forme contestataire, le fait de remettre en question un ordre établi. Je suis frappée par cette omniprésence de la télévision dans la pensée des gens : ça passe à la télé donc c'est vrai... Sur le Net on y croit moins, on se méfie... C'est que le contrôle n'est pas total... Donc le sujet se prêtait à mon propos, qui est une prise de parole du Maghreb et de l'Afrique en général pour dire qu'on existe autrement : dans la modernité aussi... Nous sommes branchés sur le Net, alors profitons-en pour passer des messages. D'autant que c'est plus facile que de créer un parti politique et c'est plus rapide pour trouver des solidarités... Je crois que la contestation peut se réfléchir autrement aujourd'hui, on le voit bien avec les mouvements alter-mondialistes... Donc à vos claviers pour la liberté d'expression ! Je pense que c'est le message du film qui finalement s'adresse à l'universel pour revenir en Tunisie...

L'informatique est un secteur masculin, ne parlons même pas du milieu sécurité informatique, hacker et pirate. Le fait qu'une réalisatrice se penche sur le sujet est étonnant, non ?

Pour moi je ne fais pas de différence... Je ne me suis pas posé la question, mais en même temps je savais que je prenais les choses à l'encontre des clichés... Mais le personnage du film, Kalt, est bisexuelle ainsi que celle de la DST qui la poursuit à travers les ondes... Je crois qu'au 3ème Millénaire on peut se permettre de dépasser le sexisme...

Quelle a été votre approche de ce sujet ?

Au départ en néophyte, j'ai écrit mon histoire et puis je me suis documentée... en surfant pas mal depuis Tunis...Mais de là-bas le Net est très contrôlé... Dès que vous allez un peu loin sur certains sites, votre ordinateur se bloque... Et puis par le biais d'autres rencontres j'ai fait la connaissance d'Edouard Tonneau... Et là, le projet a pris une autre allure. Déjà j'étais plus sûre de moi quant à la vraisemblance de mon scénario. Mais je suis toujours l'internaute moyenne !

Qui est Bedwin hacker ? Une histoire vraie ?

Non, ce n'est pas une histoire vraie... Kalt, la Pirate Mirage (car elle efface ses intrusions comme personne !) signe tous ses messages d'un petit dromadaire de dessin animé : Bedwin Hacker. Le choix du dromadaire, c'est parce qu'il est arrogant, nonchalant par rapport au temps qui passe, rancunier, et surtout parce qu'il mord alors qu'on ne s'y attend pas !

Vos sources d'inspiration pour un tel sujet ?

C'était surtout en réaction à la manipulation de l'information, à la surveillance partout des caméras nous filmant, les écoutes... Je pense que nous pouvons nous servir de cette nouvelle façon de communiquer comme d'une arme pacifiste pour lutter contre cette uniformisation de tout, qui conduit peu à peu à une anesthésie générale... La contestation est devenue illégale : un comble ! Avant, on ne voyait ça que dans le cadre des dictatures... Moi, je veux être en éveil et en réaction...

Votre personnage, Chams, semble ne pas savoir dans quel camp agir ! Comme un internaute qui peut basculer de l'état de hacker à celui de pirate ?

Chams croit qu'il est libre... Pour moi, la liberté est toujours à portée de main car on a toujours le choix de se soumettre ou de résister... Chams veut sa nationalité française parce qu'il croit que c'est ce qui le rendra libre... Il ne peut renoncer à ça, même pour l'amour de Kalt... Il a finalement choisi une autre aliénation... Oui, on peut toujours choisir les limites de sa propre morale...

Des films sur les hackers, il y en a eu quelques uns, uniquement des américains, montrant les hackers, pirates fous dangereux prêts à tout pour de l'argent. Vous ne semblez pas avoir surfé sur cette même idée, pourquoi ?

Les américains ont tendance à ériger l'argent comme valeur absolue... C'est un moteur pour certains. Je suis habitée par d'autres préoccupations, fatalement mon film montre un autre visage des hackers... Ce sont pour moi les nouveaux révolutionnaires... Ceux qui porteront la contestation avec des armes pacifistes, à la portée de tous... mais qui peuvent mettre à mal cette formidable économie mondiale ! C'est le sens des messages qu'envoie Kalt, quand elle arrive à faire éteindre les tours de la Défense...

Votre action se passe en Tunisie. A part le fait que c'est un superbe pays, est-ce un moyen pour vous de montrer que tout le monde peut être touché par cette forme d'hacktivisme ?

Comme dans tous les pays, les jeunes tunisiens surfent en grand nombre et prennent d'assaut cyber cafés et autres lieux... En Tunisie aussi il y a des internautes emprisonnés....

Pour vous, faut-il différencier hacker et pirate ?

Je ne suis pas moraliste, et parfois la frontière n'est pas évidente... Je ne suis pas sûre d'avoir un avis à ce sujet... D'ailleurs mon personnage Kalt est surnommée « Pirate Mirage »....

Imaginez-vous votre film piraté sur internet ?

Ce serait génial, ça voudrait dire que le film est apprécié !! Mais ça serait moins génial pour mon porte-monnaie, qui est déjà très vide !

L'avenir de l'informatique d'après vous ? Plus de police ? Moins de liberté ?

Certainement, mais nous n'allons pas les laisser faire !

BIOGRAPHIE

Nadia El Fani est née en 1960 à Paris d'un père tunisien et d'une mère française, et si elle a vécu son enfance à Tunis, elle a ensuite partagé sa vie d'une rive à l'autre de la Méditerranée... Nadia fait son premier stage d'assistante à la réalisation sur un film de Jerry SCHATZBERG, remake de L'Incompris de COMENCINI. Assistante à la réalisation sur des films de Romain GOUPIL, Roman POLANSKI, Franco ZEFFIRELLI, Nouri BOUZID, Alexandre ARCADI, Herbert ROSS, et bien d'autres... elle lance sa boîte de production Z'Yeux Noirs Movies et va réaliser : Pour le plaisir, Fifty fifty mon amour, Tanitez-moi ou encore Tant qu'il y aura de la pelloche.
La bande-annonce de Bedwin hacker.

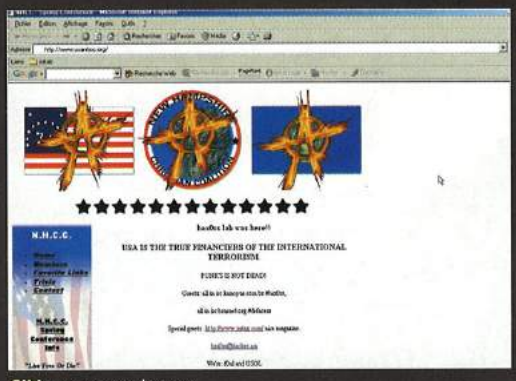
LES SITES PIRATÉS DU MOIS

Il s'en passe de drôles sur le réseau des réseaux. Voici notre sélection des sites Internet piratés soit par des scripts kiddies en mal de reconnaissance, soit par des hacktivistes ayant trouvé ce moyen pour faire passer leurs messages. Si vous aussi vous êtes témoin d'un piratage de site web, contactez-nous via contact@zataz.com.

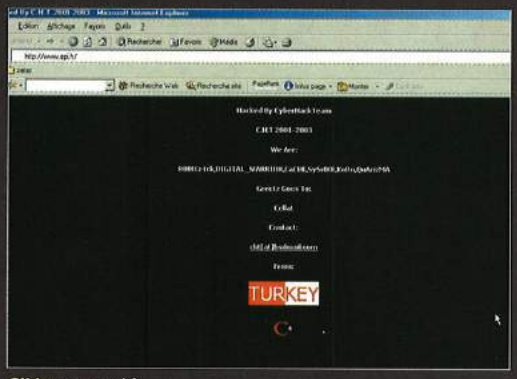
Cible : Plusieurs dizaines de sites web
Auteur : Inconnu
Commentaire : L'emprisonnement de José Bové, le porte-parole de l'anti-mondialisation à la française, n'a pas plu à tout le monde. Un pirate est allé le faire savoir sur plusieurs dizaines de sites français et belges, via une image somme toute rigolote : José Bové sur l'étiquette d'une boîte garantissant son contenu sans O.G.M.

Cible : Une centaine de sites
Auteur : Dwxr
Commentaire : Ce pirate semble avoir une haute opinion de lui-même. Ce qui est, il faut être honnête, le cas de la majorité des défaceurs. Ils ne donneraient pas leur nom si ce n'était pas le cas. Pour le petit Dwxr, le message consistait à dire « hacking is not a crime ». Le hacking peut-être pas, mais le remplacement d'une page index sans avoir été invité à le faire est un délit, un vrai.

Cible : Centaines de sites.
Auteur : Haxors Lab
Commentaire : Les plus vieux défaceurs du web d'Amérique du sud, et on vous le donne en mille, ils sont brésiliens et passent le bonjour à ZATAZ Magazine. Voilà qui est plutôt cocasse. Haxors Lab était en interview dans ZATAZ Magazine 7, voilà très certainement ce qui explique une telle chaleur de leur part !

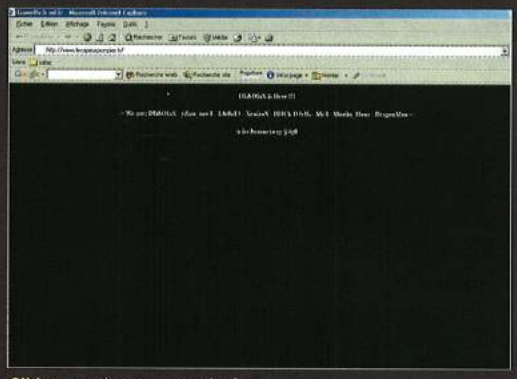


Cible : www.usanhcc.org
Auteur : Haxors Lab
Commentaire : Dans le même genre d'idée, un « nice magazine » pour zataz sur un site de l'armée US. On l'a su tout simplement ! Le webmaster du site en question nous a demandé ce que faisait le lien de notre magazine sur leur page. Vu que nous sommes des « nice people » ce n'est pas à nous qu'il fallait le demander. Rompez le rang.



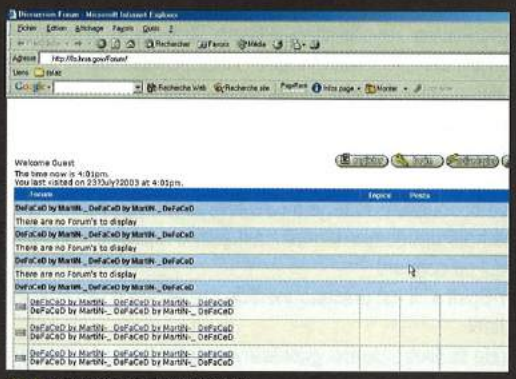
Cible : www.epi.fr
Auteur : CyberHackTeam
Commentaire : Un pirate turc, voilà qui n'est pas courant. Ce dernier semble être « actif » sur la toile depuis 2001, c'est du moins ce que l'on croit comprendre dans le piratage de l'entreprise française Epifloor. Côté message : heu ...Rien, juste « greetings » !

Cible : donation.greenpeace.fr
Auteur : Red Eye
Commentaire : Red Eye - Mr.IgNiTiOn passe par le site Greenpeace France, plus précisément via la page donation. Ce pirate avait un message à faire passer : « Salvem as Baleias, soltem a mae do ADMIN !!! ». En gros, comprenez : « sauvez les baleines et les administrateurs systèmes ». Il a oublié les idiots aussi !

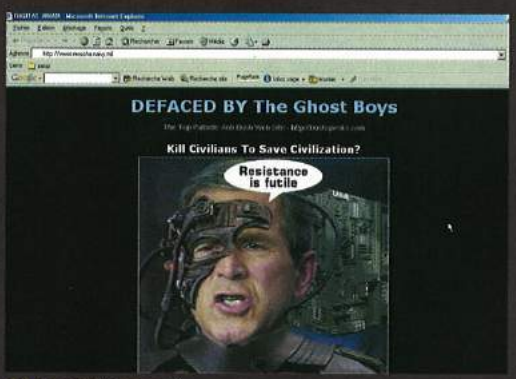


Cible : www.lesapeurpompier.fr
Auteur : DlabOlaX
Commentaire : Un pirate, DlabOlaX, est allé mettre le feu sur le site de la Fédération Nationale des Sapeurs Pompiers Français. Rien de passionnant dans le message de ce pirate : « DlabOlaX is Here !!! ». C'est gentil d'avoir pensé aux soldats du feu qui ne savaient plus où donner de la lance au moment de ce piratage. On pense cependant qu'il y avait d'autres moyens de les soutenir.

Cible : www.mairie-anceaumeville.fr
Auteur : Far[3]aS
Commentaire : Ce pirate d'origine nord-africaine est le type même de l'utilisateur de faille à script kiddies. Un forum, une faille, et chaud devant ! Le pirate propose d'aider l'administrateur en carton, comme il le nomme. Voilà le genre de discours qui ne donne pas vraiment envie de faire appel à lui !



Cible : http://fo.hrsa.gov/Forum/
Auteur : Martin
Commentaire : Certains responsables de sites appartenant à l'équipe du président George W. Bush, feraient mieux de reprendre quelques heures de formation à internet. Un forum utilisant Web Wiz sans avoir été patché, il fallait oser. L'administrateur mérite une paire de coups de pieds au c.. Un jeune idiot du village planétaire en a profité pour tout détruire. Il n'y avait pas un âne qui s'appelait Martin ?



Cible : nwschs.navy.mil
Auteur : The Ghost Boys
Commentaire : Ce groupe de pirates a décidé de prendre la relève dans la diffusion d'informations au sujet de la politique du président américain. Pour ce faire, ils sont passés par une dizaine de sites militaires de l'Oncle Sam, façon pour eux d'être certains d'être lus. A noter, en bas de page un Free DkD.

LE ROMAN DE ZATAZ MAGAZINE

NOSMAN

- CHAPITRE 1-

John Jean est un jeune auteur français qui va proposer dans chaque ZATAZ magazine un chapitre de son roman « *Nosman* ». Une exclusivité rien que pour vous.
L'histoire : « Shipper est un jeune internaute fan de hacking. Une vie tranquille jusqu'au jour où la police vient frapper à sa porte. Obligé de fuir, il va découvrir que sa passion a remué ce qui aurait du rester enterré dans les méandres électroniques du réseau ». Accrochez-vous et que l'aventure commence.

« POLICE ! OUVREZ ! »

Je me réveille en sursaut. J'hésite à ouvrir les yeux, après tout ce n'est peut-être qu'un vilain rêve. La porte commence à trembler, un mec tambourine, mauvaise hypothèse. J'ouvre les yeux en vrac. Dehors un gros bruit, des sirènes, un gars qui est en train de perdre haleine dans son mégaphone. Je comprends rien du tout. Psycho a l'air aussi étonné et apeuré que moi. On se regarde, on s'est compris. J'enfile mon froc à la barbare, laçage des chaussures façon Marines et c'est parti. Je chope le gros sac de sport, j'arrache les PC des prises murales, on n'a pas le temps de faire dans le détail. Psycho emplit le sac des CD-R gravés depuis quelques jours. Je sens que le sauvage commence à perdre patience, la porte tremble de plus en plus, assez perdu de temps, on s'arrache.

Ce squat, on y était depuis déjà deux semaines, le temps de l'arranger et déjà obligés de le quitter. Comme à chaque fois, on prévoit notre sortie de secours, là c'est le rush, on détale dans les couloirs au fond de la pièce et on atteint l'escalier de secours. Les flics ont encore bien fait leur boulot, la voie est libre, y'a vraiment des moments où je les adore. On atterrit dans une ruelle sombre, humide, qui donne sur la périphérie de la ville. C'était tout l'intérêt du squat, ne pas être trop en vue, comme en plein centre ville. L'endroit craint, on va pas s'attarder ici, on détale.
« Putain ! Mais c'est quoi ce bordel ? On s'est fait busted ? Qu'est-ce qui s'est passé ? » J'en peux plus, je souffle comme un taureau.
« Je sais pas, ta gueule et fonce, ils sont peut-être derrière nous !
- On fout quoi ?
- Plan B, on trace chez Tankian ! »

Il est bien ce Psycho, il prévoit toujours tout, il a toujours un plan B, c'est le malin et le costaud à la fois, il est impressionnant ce type. Tankian c'est le plus clean, le moins engagé dans quoi que ce soit, disons qu'il fout pas les mains dans le cambouis. Tout ce qui l'intéresse dans le hack, c'est l'exploitation d'informations. Ce mec, c'est notre passerelle à nous entre le monde réel, celui où l'on trouve le commun des mortels, et l'underground.

On a quitté la ville depuis une dizaine de minutes, on n'arrête pas de courir, mes poumons me brûlent, à tel point que je me demande s'ils se remettront un jour de cette course. L'idée c'est d'arriver chez Tankian, on y crèche une nuit ou deux, et on repart vers de nouvelles aventures. On s'arrête un peu de courir, on est dans une sorte de sentier qui longe la route, je me perds dans mes pensées histoire de ne pas compter les minutes pendant que je marche. Trois questions me hantent et me reviennent constamment : « Qui ? Pourquoi ? Comment lui faire payer ? »
On arrive enfin. Pas trop tôt, je vais m'écrouler. Je sonne une fois. Aucune réponse. Les secondes passent comme des heures. Mes mains commencent à trembler nerveusement. Je tente une seconde fois. Et là, soulagement, c'est une explosion de joie intérieure. Tankian vient d'ouvrir la porte, il est là, les cheveux retournés, l'air complètement ahuri.
« Qu'est-ce que vous foutez là les mecs ? »
Psycho le pousse sans lui demander son avis, claque la porte et se pose dans le canapé. Je fais de même et je sens déjà que la fatigue m'envahit, alors que Psycho raconte notre histoire dans les moindres détails. Tankian sue à grosses gouttes. Nous sommes désormais à l'abri. On branche les PC, startmodem dans la console et nous revoilà sur la toile. On sort les Cd qu'on a pu sauver, pas question de revenir au squat, on s'est fait débusquer. La police attend sûrement, en planque. Je m'affale dans le sofa, c'est que je n'ai pas fini ma nuit, moi. Je me suis couché il y a à peine une heure, et j'ai quasiment pas dormi depuis trois jours. Je suis simplement fatigué et j'ai les yeux qui brûlent d'avoir passé la nuit devant un brute forcing d'un pass root chopé par Psycho.

Petit tour sur les forums généraux d'abord, rien de bien net, pas de trace d'un corbeau. Un petit coup d'IRC, merde ! Personne qui puisse me renseigner, ou du moins personne de fiable auprès de qui je puisse avoir des renseignements sérieux. Pour l'instant, pause bouffe, car si j'ai pas dormi depuis trois jours, mon ventre crie famine depuis au moins aussi longtemps.
- « Vous avez failli vous faire buster alors ? mince... »
Tankian nous regardait avec des yeux tout ronds. A moitié entre l'admiration et la peur. Un frustré qui reste à la limite, il n'ose pas faire le grand plongeon dans l'under. Perso, je me suis posé comme une merde sur le canapé, entre la somnolence et l'activité cérébrale hyper développée. C'est usant, cela fait six mois que j'ai tout lâché pour m'intégrer dans la Résistance, mais je fuis tout le temps, ou alors je crèche dans des caveaux humides et miteux. Enfin, tel est notre lot. Je ne regrette rien. Quand je vois tous les lamers qui se disent hackers, je rigole. Ils ne savent pas ce que c'est. Ils se la pètent sur des chats bidons, mais n'auraient pas la moitié des couilles nécessaires. Enfin, chacun sa croix, comme dit l'autre. Psycho discute avec Tankian. Ils échafaudent des plans, je suis loin. Je capte plus rien. Je m'endors sur le sofa, ça me change des matelas à deux balles. Quand soudain, réveil de nouveau en fanfare :
« Shipper, je l'ai chopé !
- Hein ? »
J'ai les yeux bousillés, mais je me relève. Je jette un coup d'œil à l'horloge, une heure et demie de répit. Ok, je me reposerai ce week-end.
« C'est qui ce connard ?
- Hacker-Spirit ». Il est presque mort de rire en me disant ça. Je le fixe, l'air dubitatif.
« Arrête de te foutre de ma gueule avec ce mec, on en reparlera plus tard, c'est qui le blaireau qui nous a dénoncés ?
- Hacker-Spirit. Il traîne sur Hackever. »

Là je reste sur le cul. C'est le mec capable de te flatter durant 16 heures d'affilée sans complexe pour obtenir la moindre information sur un exploit connu. Hackever ? Ce truc de newbies et de blaireaux pure souche ? Comment il a pu savoir où nous squattions ? Beaucoup de questions, pas de réponse.

« Il est connecté ?
- Yep monseigneur, à toi de jouer. »

Je me relève un peu. Comme par magie, un portable glisse jusqu'à moi sur la table basse. Connexion enclenchée, les dix doigts chauds bouillants. Repéré en salon. Grande gueule. Je récupère son IP grâce à un exploit. C'est là tout l'intérêt des servers IRC : quand t'en connais un, tu les connais tous. Une petite résolution DNS suivie d'un tracer. Incroyable, il est dans la même ville que nous. Petite balade nocturne chez son FAI puis France Xocom. Griffonnage de l'adresse sur un papier.
« Tiens Psycho, son adresse. Cadeau pour ton anniversaire, sorry j'étais fauché. »

Un sourire carnassier illumine son visage :
« C'est pas grave, ça valait le coup d'attendre. »
Je me remets au boulot. Opération destruction de bécane. On se protège encore un peu, petit routage vite fait par un Proxy en Norvège, un autre au Japon. Et voilà, fin prêt.

Je lance l'attaque. D'abord, prise de contrôle de la machine distante. J'essaye deux, trois exploits. Blaireau, aucune protection, même pas un Firewall. C'est trop facile. Les petits trucs marrants de base, je t'offre un porte-gobelet, je suis resté assez lame au final, mais bon, ça me fait marrer. Bon, après l'amuse-gueule on passe à la partie destruction à proprement parler. Un petit changement de fréquence de carte mère, le balayage de l'écran boosté, et pis oups... Ton disque dur est allé chercher un secteur trois fois trop en dehors de la surface de ton ordi... Désolé. J'espère pour toi que ton écran t'avait pété en pleine gueule avant que tu n'aies pu t'en rendre compte, bichette. C'est à mon tour d'avoir le sourire carnassier. Psycho me regarde, il sait que j'ai réussi. Je ne suis pas trop pour la destruction en général. Mais là, fallait faire un exemple. Un petit tour par le salon. Tiens, il parle plus...Bizarre.
« On va l'achever ? »
Psycho me regarde, debout, sur le départ, très excité. Let's Rock !

On y va plus tranquillement que lorsqu'on s'était barrés du squat. Quand j'y pense, on a laissé du matos quand même là-bas. Perdu à jamais... Les boules. Je venais juste de trouver un accès intéressant sans avoir le temps de backdoorer...Tant pis. La prochaine fois, on sera encore plus prudents. On a laissé le matos chez Tankian, mais dès qu'on aura fini chez Hacker-Spirit on récupèrera le tout. On se rapproche, je sens que Psycho se prépare psychologiquement. Il a la mâchoire serrée si fort que j'ai l'impression qu'il va péter toutes ses dents. Il m'impressionne dans ces cas-là. C'est la deuxième fois que je le vois prêt à détruire quelqu'un. La première fois, le résultat n'était pas beau à voir. Bah ! C'est une masse ce mec, quand même...Y a pas à dire, ça se sent les quelques années de boxe derrière lui. On arrive en vue de la baraque. Chic, classe, enfin surtout pour quelqu'un comme moi qui n'a pas dormi dans un vrai lit depuis six mois.
« Merde ! J'ai peut-être pas si bien réussi mon coup que ça.
- T'inquiète pas, je vais terminer le boulot... d'une manière ou d'une autre. »
On est proches de la porte. Psycho se tourne vers moi.
« Attends-moi là, ça va pas être long. Et pis aussitôt après, on change de ville. »
Le signal était lancé. Psycho partait en guerre.

Un cri. Psycho qui hurlait. Je me serais attendu à tout, sauf à ça. Il hurlait, comme pris au piège. Un cri de bête blessée, se débattant comme elle peut. Je commençais à paniquer, je n'étais qu'à quelques mètres de la baraque, et pourtant je l'entendais comme s'il avait été à côté de moi. Je sautillais sur place. Pris entre l'envie de me sauver à toutes jambes, de détaler ventre à terre. Je suis un admin réseau, pas superman. Mais c'était mon pote qui était là en train d'hurler à la mort. C'était le seul en qui j'avais entièrement confiance maintenant. Je devais faire quelque chose. Je m'avance prudemment vers la bicoque, pas rassuré du tout, et pourtant déterminé à sortir mon pote de là. Je m'avance, et j'entends un boucan d'enfer dans le salon. Du bris de verre, des meubles bousculés dans tous les sens. Je m'active un peu. Je monte les quelques marches qui me séparent de la porte. J'attrape la clenche, au même moment la porte s'ouvre en grand. Je reste pétrifié, incapable de bouger un muscle ou de dire quoi que ce soit... Psycho me percute violemment, et on se retrouve tous les deux les quatre fers en l'air dans l'herbe. Psycho m'a sonné, je le regarde, il est couvert de sang. Il me regarde avec des yeux fous. De la bave coule de sa bouche, et sa lèvre inférieure tremble, réflexe inconscient, incontrôlé et incontrôlable.
« Psycho... ?
- CASSE-TOI ! »

Il hurle si fort que j'ai un mouvement de recul et je me trouve pétrifié à nouveau. Il me chope au col et me pousse très fort.
« CASSE-TOI ! SAUVE TA PEAU CONNARD ! C'EST DES FOUS !!! »
Ses yeux étaient terrifiés et absents, mais au fond, on sentait une étincelle de je ne sais quoi. De survie je crois. Mais pourtant...

Je commence à courir aussi vite que je peux. J'ai décidé de suivre son ordre au pied de la lettre. A une cinquantaine de mètres de la maison, je me retourne et j'entends Psycho hurler encore plus fort que ce que j'avais déjà entendu. Il était toujours dans le jardin et trois mecs étaient sur lui. Des costauds au moins aussi énervés qu'il l'était en arrivant. Ils l'ont attrapé et maîtrisé sans trop de difficultés. Malgré l'obscurité qui m'entourait, je suis certain que juste au moment où il s'est arrêté de crier, c'est-à-dire juste avant d'être porté dans la maison et que la porte ne se referme sur lui, il regardait dans ma direction. Au moment où la porte se ferma j'ai entendu un « COURS ! » aussi puissant que bref. Et puis plus rien.
J'étais hagard. Aucune lumière ne s'était allumée dans le voisinage. Je cours, me retournant, persuadé d'être suivi.

Incroyable mais vrai, arrivé devant chez Tankian, j'aperçois la police. Ils m'attendaient. Je m'arrête juste avant d'être à découvert et j'observe.
« Putain, comment ils ont fait ? Qu'est-ce que c'est que ce p..... de bordel ? ! »

Je vois Tankian, menottes aux mains, encadré par deux flics d'un genre plutôt balaise. Ils semblent sortis tout droit du film Judge Dred. Trois autres les suivent avec notre matos dans les mains. Sur le pas de la porte, les parents de Tankian. Ils sont effondrés. Comment avaient-ils pu nous repérer, surtout aussi vite ? Merde ! Je pensais qu'ils seraient passés avant par la Norvège avant de débarquer ici ! Je me trouvais sans soutien humain, poursuivi par les flics, n'ayant nulle part où crécher, et pour la première fois depuis le début de ma nouvelle vie... sans plan B.

Je devais improviser, et vite. Etude rapide des fonds de poches. Vingt euros miraculeux, vestiges de mes journées de diète. Eh bien, je crois qu'ils vont me servir. C'est le moment pour moi de changer d'air. Et vite fait. Je longe les trottoirs sombres, et je m'éloigne de la baraque de mon dernier lien avec le Monde du Milieu. Direction la gare. J'ai de la chance, il est tard, mais pourtant il reste un train.
« Où va-t-il ? » je demande au guichetier.
- Il part vers la pointe du raz.
- Ok, ça fait combien ?
- Treize euros, 3 heures 30 de voyage.
Alors à 2 heures du matin, avec sept euros en poche, je monte dans un train qui m'emmène vers un coin paumé de la France profonde. Dans ma tête, les cris de Psycho résonnent, se mixant malignement avec un « Cours Shipper ! » d'encouragement à mon attention.

A suivre ...

COURRIER

Une remarque, un commentaire, une question ? Le courrier des lecteurs vous est ouvert. Nous ne pouvons répondre à toutes vos missives sur cette page mais nous répondons à vos mels en 8 heures chrono ! N'hésitez pas à nous écrire via zataz.com

Teuf ! Teuf !

Bonjour,
Tombé dedans assez tard (48 ans et j'en ai 51), je découvre le monde magnifique de l'informatique. Désireux de progresser, je me documente et je suis un lecteur assidu de votre magazine depuis sa parution. Ce courriel est motivé par une question : Dans votre numéro 7, page 24, vous parlez de Linux-Knoppix. Depuis quelque temps, avec les déboires que je connais à cause de Windows, je m'intéresse à Linux. Ma question est la suivante : où peut-on trouver le CD en question, sans avoir à télécharger ce programme ? Avec un vieux modem 33600 et 10h par mois, je suis plutôt limité côté internet.
(BOUHL JC par mel)

D'abord merci pour votre fidélité ! Pour ce qui est du Linux - Knoppix il n'est malheureusement disponible que sur internet, et effectivement avec un modem 33 600 bauds vous risquez de mettre pas mal de temps pour le télécharger. Pour en savoir plus, et télécharger gratuitement ce logiciel, rendez-vous à cette adresse : http://www.zataz.com/zatazv7/news.php?id=2725

Wanted !

Salut !
Tout d'abord, bravo pour votre mag, il est clair, simple et en plus en couleurs. Je voulais féliciter le concepteur du logiciel logP2P contre la lutte de photos ou vidéos mettant en scène des mineurs sur le réseau P2P. Pour ma part, j'étais un adepte du P2P, mais malheureusement j'ai dû arrêter car il m'est déjà arrivé de charger des photos et des vidéos, dont le titre n'avait rien à voir avec le contenu. Bien évidemment je les ai supprimées, mais c'était déjà trop tard. Il est fort dommage que le P2P soit pollué par ce genre de fichiers, car cela contribue à donner une mauvaise image du P2P. Je voudrais savoir auprès de qui je dois me renseigner pour avoir une adresse sur les brigades de recherche du web, car je voudrais moi aussi intégrer une équipe qui combat ce genre de choses. (scude idule par mel)

Le P2P est une excellente idée qui a été littéralement « pourrie » par les pirates et autres pédophiles. Pour ce qui est des « brigades » de recherche, il en existe de deux sortes : La police nationale, il vous faudra donc passer le concours de police (gardien de la paix, sous-officier ou officier) ; ensuite vous pourrez intégrer une section informatique. Si la gendarmerie vous tente plus, là il faudra carrément sauter dans les rangers. Dans les deux cas, allez dans un commissariat pour en savoir plus et retirer les documents sur le sujet.

Il voit des ZATAZ Partout

Hello,

Je suis un lecteur du site, qui me promène du côté de l'Equateur. Pour mon travail je voyage pas mal et j'ai trouvé ici, mais aussi au Bangladesh, des cdroms pirates contenant Windows Xp, le dernier Norton et... le ZATAZ firewall. J'ai trouvé ça dans un boui-boui du coin de la rue, sur un cd compile nommé « hacker », soit tout et rien en général.
Je suis à Guayaquil, Equateur, et j'en profite pour vous envoyer la photo d'un panneau d'affichage
MiKE par mel.

On lui a répondu par mel, mais son courrier méritait de passer dans le magazine. Surtout la photo. Faut pas se tromper une fois qu'on est en face de cette dernière !

N°1

de la presse Internet francophone

www.netscope.org

EUROPSX

REFROIDIT LES CONCURRENTS!
LA QUALITÉ À PRIX GELÉS

FRAIS DE PORT OFFERT
LIVRAISON SOUS 48 HEURES
RÉPONSES EN 24 HEURES
SUIVI DE TA COMMANDE
PAIEMENTS SÉCURISÉS

A BIENTÔT SUR EUROPSX.COM