Piratage - Virus - Sécurité - Hacking - Phreaking - Carding - SPAM

ZATAZ MAGAZINE

n°2 Avril - Mai - Juin 2002

Du DivX sur Gameboy ? Découvrez comment la GBA peut lire de la vidéo !

2€

Piratage de films

Les vrais réseaux clandestins

M6net sauvé par un hacker

CCCF Le club chasseur de pirates

BADTRACK

Le virus qui peut détruire Internet !

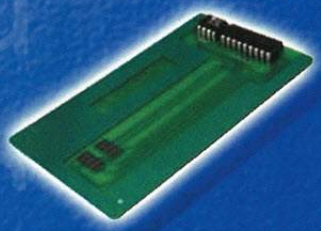
M 05129 - 2 H - F: 2,00 € - RD

Trimestriel - Belgique : 2,3 Euros - Suisse : 4,00 CHF - http://mag.zataz.com

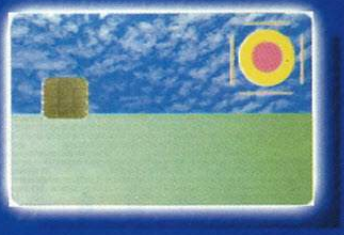
europsx.com

ARRETEZ D'ACHETER TROP CHER !!

Cartes-Programmateurs-Composants-Modchips



WaferCard
- 16F84
- 24LC16
- Supports à souder



FunCard v2.0
- AT90S8515
- 24LC64

GoldCard
- 16F84
- 24LC16

SilverCard
- 16F877
- 24LC64

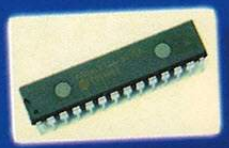
"N'attendez rien du Père Noel !

Les cadeaux sont sur europsx.com"

Puces
modification
- PSX, PSOne, PS2

Pièces détachées
- PSX, PSOne, PS2
- Blocs optiques
- Alimentation

europsx
Distributeur
Officiel
Messiah



Composants
- Pic 16F84A
- 24LC16
- Pic 16F876
- Pic 12C508
- Programmateurs
- ...

Pas de frais de port - Pas de minimum de commande
Paiement sécurisé CB
Plus d'infos: info@europsx.com ou www.europsx.com

n°2

Sommaire

EDITO

EDITO

Hello cher lecteur, voici déjà le numéro 2 de ZATAZ magazine ! A la vue de l'impressionnante quantité de courriers reçus, le magazine vous a plu et nous allons donc continuer dans la même veine que le numéro 1. Cela dit, il est bien sûr évident que nous avons pris en compte chacune de vos remarques notamment sur la difficulté à vous procurer le magazine. Kiosques dévalisés pour certains, d'autres non approvisionnés, nous avons cette fois mis les bouchées doubles pour être sûr que chacun puisse trouver un exemplaire. Impossible donc de passer désormais à côté de Zataz Magazine !
Toutefois, nous avons pris nos précautions en mettant également en place une offre d'abonnement particulièrement alléchante, comprenant en plus un CD offert.
On ne pourra pas dire qu'on ne fait pas d'efforts pour nos lecteurs, surtout aux vues du sommaire de ce nouveau numéro !

P.S. : Si vous avez envie de participer à ZATAZ Magazine, n'hésitez pas à nous contacter par e-mail : taz@zataz.com. A noter aussi qu'une partie vous est réservée sur notre site web - zataz.com.
Pour vous y rendre, il vous suffit de taper comme adresse mag.zataz.com

Damien Bancal

une publication

MEDIA Stone

http://mag.zataz.com

Zataz Magazine 61, rue Jouffroy d'Abbans, F-75017 Paris , Fax : 01.40.53.86.44 magazine@zataz.com

Chef de la rédaction : Damien Bancal
Ont collaboré à ce n° : Benoit Guignard, Eric Romang, Antoine Santo, LaurentZ, Geek Girl, Jasper, Webmaster guerreco.com
Merci à ARTCH et Christophe GAUTHIER pour leurs créations graphiques.

Impression Leonce Deprez, Béthune
Distribution : NMPP **N° de Commission paritaire :** En Cours. Dépot légal à parution.

Magazine édité par : Mediastone
Directeur de la Publication : Charles Daleau
Siret : 42990015200019 -
Code APE : 221 E

Toute l'actualité du hacking et du piratage !

actu!

Planète Underground

SABOTAGE ROYAL

La famille royale hollandaise a eu l'idée de vouloir chatter sur le web avec des internautes. L'idée, plutôt sympa, mettre en relation l'héritier du trône hollandais avec une centaine d'internautes triés sur le volet. Le problème est que des pirates ont attaqué le pauvre Prince Willem-Alexander à grand coup de DoS. Trois milliards de hits ont été enregistrés, obligeant l'hébergeur du chat, la société KPN, à couper la communication. Pourquoi tant de haine ? Le Prince s'est marié avec la fille d'un ancien ministre du général Jorge Videla, dictateur argentin. Celui-ci aurait fait disparaître plus de 10.000 personnes entre 1976 et 1981...

CANAL PLUS DÉCHIFFRÉ

Il a signé de son pseudo, Over Kill et a réussi à modifier une page du site de Canal Plus en jouant avec un questionnaire. Il a posé la question suivante dans la partie - C mon opinion - sur le site de C+ : "Overkill-a-t-il hacké canal plus ?". Les responsables du site contacté ont réparé dans l'heure en nous précisant que cette page était fermée au public.

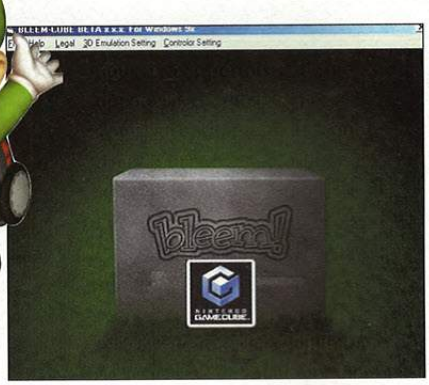
HACKERS, PIRATES, GARE AUX BOMBES

Le gouvernement des Etats-Unis a averti qu'il pourrait agir de manière militaire à l'encontre des terroristes informatiques. En gros, hackers, pirates et script Kiddy pourraient voir un jour débarquer Rambo dans leurs chambres avec un gros canon. Un conseiller de la Maison Blanche, Richard Clarke, le monsieur technologie, a même été dire que les USA "se réservent le droit de répondre de n'importe quelle manière "appropriée" pour contrer les guerriers de l'Internet." Ca va être joli un missile Tomahawk sur la cheminée.

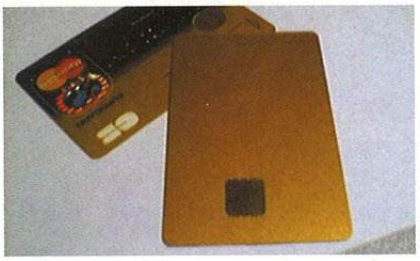
Emulateurs piégés

La nouvelle avait fait l'effet d'une bombe dans le milieu de l'émulation : un programme venait en effet d'être lancé sur Internet, permettant de clôner la console XBox de Microsoft sur un simple PC équipé d'une carte 3D. Hélas, après avoir vérifier cette information, nous nous sommes rendus compte que cet émulateur n'était rien de plus qu'un piège à gogo. Un fichier en l'occurence, Xbox.vxd nous a permis de découvrir qu'il ne s'agissait simplement que d'un bout de code du jeu «Wolfenstein». Encore plus pitoyable, les auteurs de cette supercherie se sont même pris la peine, histoire de rendre crédible leur action, de créer par un montage douteux une lettre de menace de poursuites juridiques signée par Microsoft.

Quelques jours plus tard, nous apprenons cette fois la sortie d'un émulateur Gamecube, dont la rumeur de sortie datait déjà du mois de décembre 2001. Après nos recherches habituelles, il s'agit aussi d'une supercherie...On se demande vraiment quel intérêt ont les auteurs de ces faux émulateurs à se donner tant de peine !



Yescardeurs arrêtés

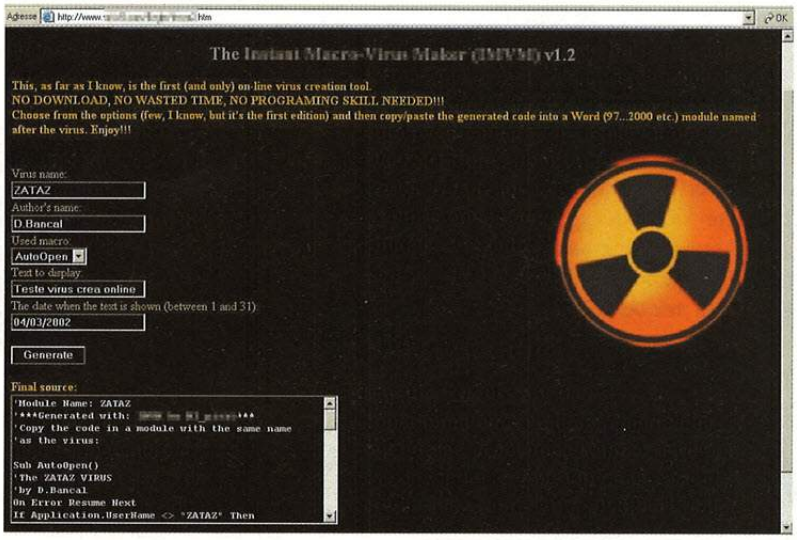


Quatre jeunes délinquants de la région de Dijon ont été arrêtés en possession de clônes de cartes bancaires. Ils ont été appréhendés après avoir attiré l'attention du personnel de l'hôtel dans lequel ils logeaient au moment du règlement de leurs chambres avec une fausse carte bancaire. Agés de 17 à 28 ans, connus de la police pour vols et drogues, ils ont été pris la main dans le sac et reconnus coupables de transactions frauduleuses. Ils avaient déjà pu acheter des vidéos, faire des pleins d'essence et régler des notes d'hôtel. Comme nous vous l'indiquions dans notre premier numéro de ZATAZ Magazine, la police a déjà arrêté près d'une trentaine de chercheurs liés à la Yescard, ainsi que des utilisateurs dans la région parisienne, lensoise, toulousaine ou encore dunkerquoise.

Sulfnbk, le faux virus

Voilà plus d'un an et demi que des messages d'alertes annoncent qu'un virus nommé *sulfnbk.exe* envahit les ordinateurs sous Windows. Pas de panique, ces messages sont des hoaxes, des canulars. Le logiciel sulfnbk.exe se trouve effectivement dans tous les systèmes d'exploitation Windows vu que ce programme est obligatoire pour faire fonctionner vos machines. Si vous tenter de l'effacer, votre machine plantera inmanquablement !

Virus Online



On en découvre de belles sur le web ! Dernière découverte en date, un site proposant de vous fabriquer en temps réel un virus pour Word. La bestiole, que l'on nomme plus communément Macro Virus, n'a rien de bien méchant, mais le site vous propose de le fabriquer en trois coups de souris. Plus besoin de connaître la programmation ou de télécharger un générateur de virii. Des irresponsables qui n'ont pas compris la leçon du virus Kournikova. A mettre ce genre d'arme entre les mains des boutonneux du web, il ne faut pas s'étonner que les législateurs souhaitent transformer le web en prison dorée. Les auteurs de cette page proposent plusieurs options comme le choix du jour de l'activation du virus et il ne reste plus qu'à copier/coller le code fourni.

La blague débile du numéro

C'est l'histoire d'un nerd qui reçoit sa feuille d'impôts et qui envoit en réponse une lettre à son percepteur qui dit:
To: (percepteur@finances.gouv.fr)
Subject: unsubscribe
Text: Veuillez retirer mon nom de votre mailing list.

De l'ANPE à la Prison

Un ancien administrateur système de la société Omega engineering a été condamné à 41 mois de prison et à plus de 2 millions d'euros d'amende pour avoir piraté son ancien employeur.

Tim Lloyd, est loin d'être un naïf bidouilleur. Déjà l'année dernière, il avait été reconnu coupable d'avoir caché en mai 2000 un virus à retardement dans un serveur d'Omega, serveur qui centralise les robots industriels de cette société. Le 31 juillet 1996, ce code viral a détruit tous les logiciels qui dirigeaient les machines industrielles de la société. Bilan, 2 millions de dollars pour la nouvelle programmation des robots et 80 licenciements pour compenser les pertes.

JUGEMENT

Six informaticiens qui vendaient par Internet des logiciels copiés illégalement entre 1996 et 2000 ont été condamnés le 14 février 2002 par le tribunal correctionnel de Paris. La plus forte peine, 6 mois d'emprisonnement ferme, a été prononcée à l'égard d'un employé de mairie qui avait vendu 4 à 5000 CD-Roms pour un total de 12 196 Euros. Des peines de 3 mois d'emprisonnement avec sursis ont été infligées aux autres vendeurs. (Source : Me M. Cahen)

PIRATAGE BANCAIRE

Plus de 5 pour cent des consommateurs en ligne américains ont eu des problèmes l'année dernière. 5% de victimes de fraude à la carte de crédit qui a représenté plus de 1 dollar pour 100 dollars dépensés sur Internet d'après la dernière étude Gartnetg2. 1,9 % des personnes interrogées ont vu leurs identités détournées. Sur près de 62 milliards de dollars de transactions, 700 millions ont été détournés par des pirates.

I.E. ET LES PIRATES

La société hongroise IVY vient de mettre la main sur une nouvelle faille de sécurité qui touche Internet Explorer et le langage XML. Lors de la conception d'un composant XML, les ingénieurs de IVY ont découvert qu'il était possible d'utiliser Internet Explorer pour permettre à un pirate de placer un code malveillant sur l'ordinateur d'un internaute. En gros Internet Explorer se transforme en Trojan. Voilà qui va faire plaisir à Bill Gates.

ECOLE ANTI PIRATES

La première école européenne de formation contre le cyber crime vient d'ouvrir à Liverpool. Cette école va apprendre aux policiers comment découvrir, par exemple, des traces et autres preuves numériques. Jusqu'à 500 investigateurs pourront venir se former, chaque année, dans la lutte contre le crime informatique incluant l'espionnage des données, la fraude à la carte de crédit, la pornographie touchant les enfants ainsi que le terrorisme.

actu!

Toute l'actualité du hacking et du piratage !

Planète Underground

PIRATAGE À TÊTE DE GONDOLE

Le directeur d'un hypermarché Cora de la banlieue de Strasbourg (Bas-Rhin) a été mis en examen par le tribunal de grande instance de Strasbourg pour introduction frauduleuse dans un système informatique, faux et usage de faux et tentative d'escroquerie. Cet homme aurait pénétré le réseau informatique de la mairie de Strasbourg afin de donner des consignes en usurpant l'identité de Fabienne Keller, maire de Strasbourg, au représentant de la Ville pour l'extension de sa «boutique» avec une galerie marchande.

PIRATE DE DVD

Cela devient n'importe quoi. Jon Lech Johansen, alias DVD-Jon, est poursuivi aujourd'hui par son pays pour avoir créé le programme DeCSS. Pour mémoire, ce logiciel permet de faire une copie d'un DVD. DVD-Jon était mineur lors de la création de ce programme. Aujourd'hui il a 18 ans et la justice norvégienne a donc décidé de le poursuivre pour... vol de données. Il risque deux ans de prison.

DRINK OR DIE

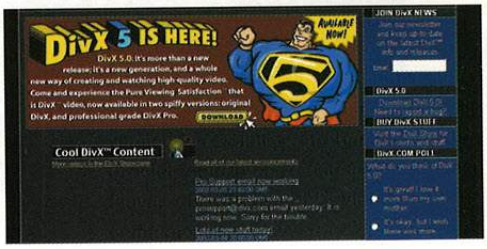
Kentaga Kartadinata et Mike Nguyen, les deux principaux membres de DoD viennent d'être inculpés de violation du droit d'auteur pour avoir copié puis échangé sur Internet des films, des jeux vidéo et des logiciels. Le groupe Drink or Die a été démantelé le 11 décembre dernier lors d'une opération internationale appelée "Boucanier". La police avait saisi plus de 200 disques durs contenant warez, Divx, Mp3, ... Les deux californiens risquent 5 ans de prison et surtout le remboursement des logiciels et films copiés. Bonjour la note !

JEU CONCOURS !

Le site de la Twenty Century Fox a eu un problème pour garder secret les Informations concernant les internautes venus jouer à son jeu "La revanche d'une blonde". Avec un simple url il était possible d'accéder au fichier des participants avec nom, prénom, adresse, ... Nous avons contacté les responsables du site qui ont corrigé rapidement le problème. Rappelons que la loi punis les sociétés qui ne prennent pas suffisamment de mesure pour protéger les informations fournies par les internautes.

Tchi Tchaaaa !

Le moyen de compression DiVX, qui permet, entre autre, de faire une sauvegarde sur CDROM des films que vous avez acheté vient de sortir une 5ème version accessible gratuitement sur le site officiel de DiVX. A noter que le lecteur Playa, qui lit, les DiVX vient de sortir sa 6ème monture. www.divx.com/divx



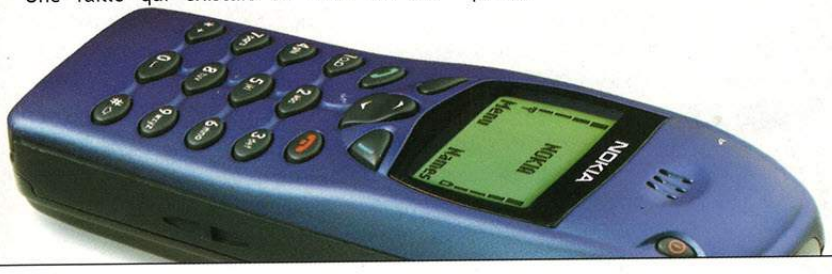
Virus pour .NET

Elle aurait 17 ans, se nommerait Gigabyte. Origine probable : Pays de l'Est, du côté de la Hongrie. Cette jeune codeuse aurait proposé à une société éditrice d'antivirus un code viral visant le langage de la plate-forme de Microsoft .NET. Le virus, nommé Sharpei est écrit en C-Sharp le code de .NET. Cette "créatrice" de virii a déjà fait parler d'elle en juillet 2001 avec un ver nommé Parrot. Son groupe, l'un des plus actifs de la scène virii édite un Ezine qui propose les dernières technologies en matière de microbes électroniques. Le virus .NET a été mis en ligne par Gigabyte le 11 janvier dernier. Nous avions pu accéder à ce virus à l'époque. Il est divisé en 3 sous-parties nommées goat2.exe, goat.exe et dotnet.exe. Les antivirus brillent de mille feux si vous tombez dessus !

Un virus dans l'oreille

Le 17 janvier dernier des chercheurs en Hollande ont découvert un bug dans le système d'exploitation employé dans les téléphones mobile de la marque Nokia. Un pirate informatique pourrait exploiter ce trou de sécurité en envoyant un message SMS - le message électronique, formé d'une certaine manière, d'environ 160 caractères serait capable de planter le système d'exploitation. Une faille qui existait en 1999 sur les téléphones Ericsson.

En Chine aussi une découverte intéressante : un bug dans le programme embarqué des téléphones Siemens permet de détruire les modèles 3568i à distance. Ce bug de sécurité rend inopérant un téléphone en envoyant un message SMS mal formé en chinois. Le "défaut", ne semble pas toucher les versions 6688. En gros, un Denial of Service dans la poche.



Lisez du DivX Sur GBA !

Des pirates chinois ont transformé la GameBoy Advance en lecteur de DiVx. Nous pensions impossible un tel exploit. On savait pourtant que la petite dernière de Nintendo, en attendant la GameCube, était capable de bien des choses ! La Gameboy Advance peut donc être transformée en lecteur vidéo. Des pirates chinois ont ainsi réussi à coder un extrait de film pour montrer leur savoir-faire. Du DiVx sur GameBoy Advance, il fallait y penser ! Nous vous proposons dans la page dédiée aux lecteurs du magazine - mag.zataz.com - une démonstration des capacités de la bestiole avec la bande annonce du film Ice Age. Il semble que les pirates ont utilisé la technologie française 4x technologies «4xtechnologies.com». Vous pouvez apprécier la démonstration grâce à l'émulateur de GBA nommé VisualBoyAdvance.

Traceur anti-pirate

L'objet à une étrange forme, il est transparent et bardé d'électronique. Son but, retrouver une personne enlevée grâce au système GPS embarqué. La société ADSX, basée en Floride, a mis en service ce traceur pour que ce dernier puisse protéger les hommes d'affaires qui sillonnent l'Amérique du Sud, région du globe ou les enlèvements sont monnaie courante. (Ndr : Plus de 3.000 enlévements par an rien que pour la Colombie selon le departement de la Justice US).

DANGER

Gla... gator

Attention, si vous faites partie des 10 millions utilisateurs du logiciel Gator, prenez-garde ! Ce logiciel qui accompagne souvent d'autres programmes gratuits comme Audiogalaxy, permet de remplir automatiquement des formulaires sur des pages web. Le problème vient d'un contrôle Active X, découvert par le site Eyeonsecurity.net, qui permettrait à quelqu'un de mal intentionné de prendre le contrôle de votre ordinateur via ce backdoor. Vu que Gator n'est pas franchement un programme indispensable, nous vous conseillons de le désinstaller tout de suite, ou bien de vous rendre à l'adresse http://mag.zataz.com pour télécharger un correctif.

A LIRE !

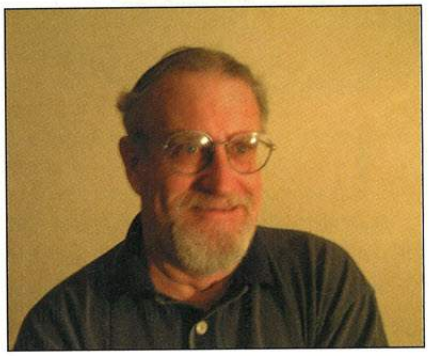
Nous avons reçu, et lu, le livre de Didier Godart : Sécurité Informatique - Risques et Solutions - aux Editions CCI. Le livre relate en 334 pages les diverses méthodes employées par les pirates et les divers outils qui peuvent permettre de les contrer. Passionnant, vous aurez de quoi lire ce mois-ci. Prix : 36 Euros. Vous avez été nombreux à nous demander le nom de notre livre, sorti en septembre 2001. « Hackers et pirates sur Internet », aux Editions Desmaret. Nous vous proposons une librairie géante sur zataz.com

ZATAZ.NET

Une partie de l'équipe de ZATAZ Magazine, aidé par des lecteurs, passionnés par la programmation, vient de lancer une section programmation via l'adresse ZATAZ.NET. Cette section est gérée par Eric Romang. Vous y trouverez des informations techniques liées à la sécurité informatique ainsi que des articles sur les Serveurs Web et les bases de données IDS (NIDS et HIDS), Apache - PHP - Mysql base, Tunneling, SSL, ... Des dizaines d'articles pour utilisateurs avancés de Windows et de Linux.

actu!

John Draper, le père du piratage téléphonique



Début des années 70, à partir d'un simple sifflet en plastique trouvé dans un paquet de céréale Crunch, Draper pirate un téléphone. Comment est-ce possible ? La tonalité du sifflet était la même que celle utilisée par AT&T pour ouvrir la ligne à un appel téléphonique. Une tonalité devenue mythique aujourd'hui, le 2600Hz. Ainsi, en émettant cette tonalité, John Draper avait accès à la ligne avant même de payer. Draper, qui prendra comme nom de guerre underground, C'ptain Crunch, sera l'un des membres du groupe *Homebrew Computer Club*. LE HCC inventera, entre autre, la «blue box», dispositif électronique pour ne pas payer le téléphone. Pour mémoire, l'un des autres membres de cette fine équipe, Steve Wozniak, n'est autre que le cher papa d'Apple. Nous avons posé quelques questions à John Drapper aka C'ptain Crunch :

Qui est John Draper ?
C'est moi :) Un vieux bonhomme avec encore pleins de projets.

Qui est capitaine Crunch ?
C'est moi également. (NDL : Capitaine Crunch est le père du piratage téléphonique.)

Que pensez-vous du Web d'aujourd'hui ?
Il est de plus en plus grand et il est aussi de plus en plus confus.

Et l'underground ?
Il reste sympa (NDLR : ouf!). En espérant qu'il va continuer à coller à l'esprit du web.

Qu'est que votre CrunchBox ?
C'est un boîtier qui va permettre de contrer les pirates. Il bloque les IP malveillants, permet de tracer un pirate.
http://www.shopip.com

Pourquoi avoir crée le CrunchBox ?
Parce que trop d'internautes, mais aussi trop de mes clients sont piratés. Voilà une bonne protection. CrunchBox est aussi une arme contre le peu de fiabilité des produits Microsoft.

Quel est votre meilleur souvenir sur le web ?
Quand j'ai mis mon premier site Web en ligne. J'étais en Inde.

Et votre pire souvenir ?
Il ne concerne pas sur le web, mais c'est quand on a volé mon ordinateur portable dans lequel j'avais mis ma vie en ligne pour un éventuel livre.

Planète Underground

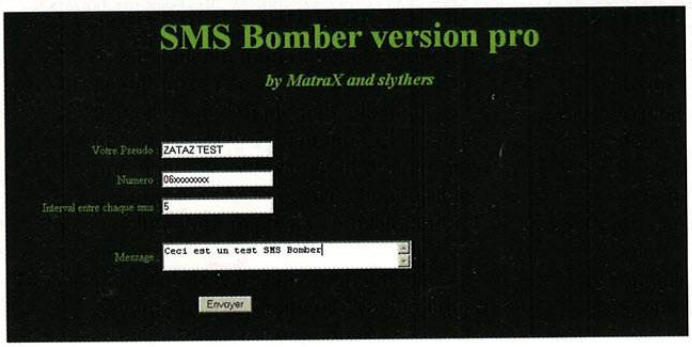
CODE RED SOUS PHP ?

C'est seulement une question de temps avant qu'un ver ne soit créé pour exploiter les défauts nouvellement découverts dans le langage PHP. Voilà une annonce que viennent de faire des experts en sécurité. Avec des millions de sites Web exposés, la faille pourrait faire comme Code Red, une belle pagaille! David Dittrich, Ingénieur sécurité à l'Université de Washington, a souligné que ce virus pourrait apparaître très prochainement sur la toile. Méfiance !

OUSSAMA SE CACHE SUR LE WEB

De nouvelles informations, émises par le Pentagone, affirment que les membres du réseau Al-Qaïda utilisent le Web pour se regrouper au Pakistan. Internet permettrait aux terroristes de se contacter sous couvert d'anonymat, n'importe où dans le monde. Juste un détail, comment font-ils pour se donner rendez-vous dans un espace inconnu sur le réseau, ils s'envoient un SMS ?

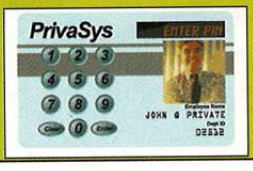
Un bombeur de SMS !



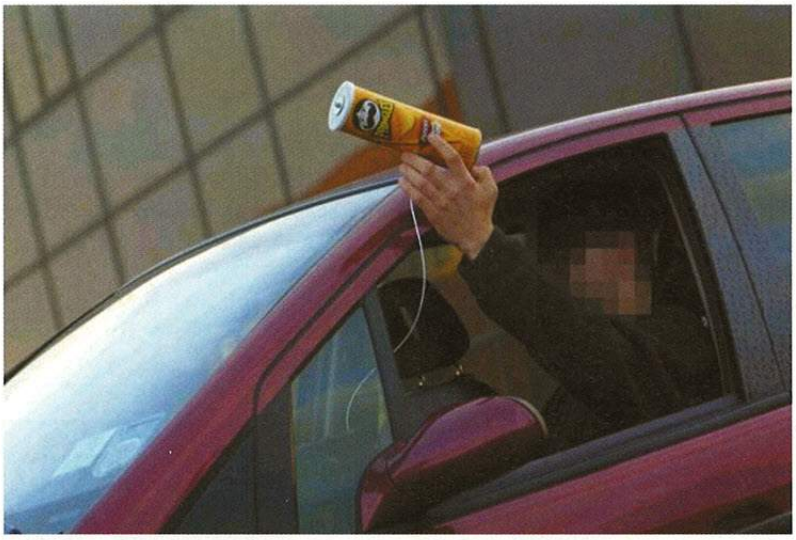
On n'arrête pas le progrès. Deux jeunes français viennent de mettre en ligne un site web pas comme les autres. Celui-ci proposait de bombarder un téléphone mobile de messages SMS, les célèbres textos qui plaisent tant aux djeun's. Le principe était malheureusement très simple. Un numéro de téléphone, votre message, le nombre de SMS à envoyer et la durée entre les émissions de message.

La CB qui intègre un clavier

On n'arrête pas le progrès. On nous propose maintenant une carte bancaire intégrant un clavier numérique pour augmenter la sécurité des transactions bancaires. Allez hop, pourquoi ne pas carrément se trimballer son micro !
http://www.privasys.com/Prod_AuthCard.htm

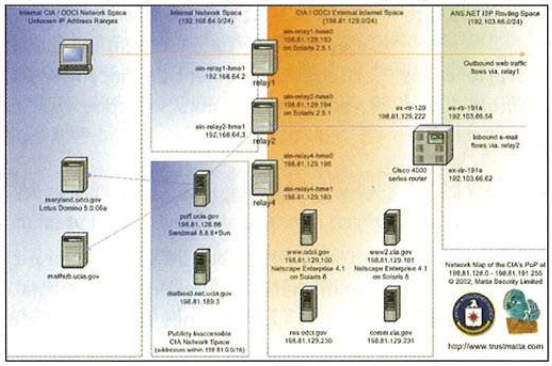


Des chips pirates



Nous ne savons pas qui est le responsable marketing de la marque Pringles, mais ce dernier doit se frotter les mains. Il semble qu'avec les boites rondes de cette marque, il soit possible de fabriquer un canon voleur de connexion sans fil. La société i-seconde a construit une antenne directionnelle employant une boite de Pringles qui a permis d'améliorer les chances de trouver les réseaux d'ordinateur sans fil. Nous connaissions la même technique avec une boite de balle de tennis ou encore une bouteille d'eau recouverte d'aluminium.

La CIA en poster dans ta chambre



La société de sécurité informatique Matta vient d'expliquer qu'elle avait cartographié le réseau informatique de la C.I.A. Le dirigeant de Matta a expliqué que ses collaborateurs s'étaient uniquement basés sur des moteurs de recherche publics. Domaine, sous domaine, Ip, numéros de téléphones, ... Bref une cartographie sympa pour les espions en herbe. Marrant comme information, surtout après l'annonce de la mise en place d'un bureau des «mensonges» par le Pentagone.

On s'emmmerde pas !!!

Un site porno piége l'armée américaine en utilisant sa bande passante. Gilbert Benjamin, 49 ans, webmaster de sites pornos, a carrément squatté la bande passante de l'US Army pour mettre en ligne ses sites pour adultes. Il a utilisé le réseau haut débit en faisant croire qu'elle servait à la communication avec les forces armées basées en Bosnie. Il a été arrêté ce jeudi à New Jersey.

UN HIC DANS LE ZLIB

Une faille a été découverte dans la librairie nommée Zlib. Ce petit programme permet de décompresser les librairies utilisaient par l'Os Linux. La vulnérabilité, mise en avant sur Slashdot, peut faire planter votre machine quand zlib décompresse certaines données. Vu que zlib est partout, imaginez le problème.

SPY WAR

Selon une analyse du trafic réseau exécutée par Eeye Security, le navigateur Netscape a d'étranges manières. Il semble qu'AOL, propriétaire de Netscape, intercepte les requêtes de recherches des utilisateurs. En gros, une base de données des recherches est en train de se fabriquer sur le dos des internautes. Les données sont envoyées vers le serveur info.netscape.com

AH LES CONS !

Plus de 3.000 Pakistanais ont tenté via Internet de demander la nationalité Ladonienne. Le seul hic est que Ladonia est un pays virtuel qui se situe dans le sud de la Suède et grand d'un kilomètre carré. C'est un artiste, Vilks Lars, qui avait inventé ce pays imaginaire. http://www.aim.se/ladonia

.KID POUR LES KID

Un jury du congrès Us vient de donner son accord pour un projet de loi qui instaurera le fait que les sites en .kid seront autorisés au moins de 13 ans. Une sorte de zone où les gamins ne tomberont pas sur des sites pornos, de jeux d'argent, de violence. Voilà une très bonne idée. En espérant que cette zone ne se transforme pas en supermarché pour gosse comme savent si bien le faire les sbires de l'Oncle Sam.

PROTECTION DE CD

Midbar, société nippone, vient de mettre en service un système de protection de CD. Un système qui permettrait de contrer la reproduction du contenu numérique sur ce support. La société explique que les CD sont protégés via certaine partie du rond de plastique. En 2000, la société BMG avait testé la protection de Midbar sur 100 000 CD.

Focus

Bad Track, le virus qui peut

Un ingénieur en sécurité informatique met la main sur un code viral qui fait frémir les pros du Web. La raison en est simple : une fois propagé, ce virus peut tout bonnement paralyser l'intégralité du Web, soit des centaines de milliers de serveurs. Après réflexion, et l'autorisation reçue de l'inventeur de ce code viral, Zataz Magazine vous livre en exclusivité les dessous de ce dossier brûlant.

Vincent Royer est ingénieur en sécurité informatique et travaille dans l'entreprise d'expertise Althes basée dans le nord de la France. Son métier consite à réaliser des tests d'intrusion sur des serveurs pour le compte de grandes entreprises pour détecter leur fiabilité. En novembre 2000, lors d'un test d'intrusion, il découvre par hasard une faille et se met à l'éprouver : «la faille a l'air très simple à utiliser par des pirates, le risque a l'air très grand».

Rentré chez lui, il réfléchit au fait que cette faille, couplée avec un système efficace de propagation pourrait rapidement infecter 60% de tous les serveurs web en seulement quelques heures. Vincent Royer a entre ses mains une bombe à retardement.

«Un pirate qui se mettrait en tête d'infecter un moteur de recherche infecterait toutes les personnes qui s'y connecteraient. Pas de pièces jointes à ouvrir, une simple consultation du site infecté les contamineraient automatiquement !

Vincent prend conscience de la gravité de sa découverte et en fait une démonstration à son patron qui en restera pantois. "Là je flippe !", lâche instantanément son employeur, "surtout que ce code ne dépasse pas les 1 000 caractères !». Vincent, le père de ce virus le baptisera «Bad Track», pour une raison qu'il préfère garder pour lui.


Vincent Royer, dans son bureau.

« Tous ont été unanimes : notre code était vraiment dangereux»

Les experts aux abonnés absents

Cet ingénieur aurait-il découvert la boîte de Pandore du web ?

Ni une ni deux, il contacte la Direction Centrale de la Sécurité des Systèmes d'Information (D.C.S.S.I.), une cellule militaire attachée aux services du premier Ministre. Il veut savoir s'il a découvert une réelle menace pour Internet ou une simple chimère. «Je leur ai donc envoyé le code viral, une partie par e-mail et l'autre par fax ». Pendant trois mois, Vincent Royer et la société Althes n'ont aucune nouvelle.

Ils recontactent alors cette structure attachée au secrétariat général de la Défense Nationale : «Ils nous ont d'abord expliqué que notre code était à l'étude et que finalement, notre découverte n'était pas importante du tout».

Ces experts de la défense indiquent même qu'il n'y a aucun risque! Etonnement de Vincent Royer, qui, persuadé de sa découverte, envoie alors son code viral à plusieurs sociétés éditrices d'antivirus. «Tout de suite le ton a changé. Les réponses ont été immédiates !» Tellement immédiates que le PDG d'une de ces sociétés américaines (que nous ne pouvons citer pour clause de confidentialité), alors en vacances, téléphone en urgence à la société Althès. «Il a contacté de nombreux experts qui ont tous été unanimes : ce code était vraiment dangereux. Il a affirmé qu'en quelques jours ce virus, Bad Track, pourrait infecter le web entier.»

Le PDG reste tout de même prudent et précise à Althès qu'il ne leur a jamais rien dit à ce sujet. On navigue alors en plein James Bond !

Même pas peur !

Que faire ? D'un côté une cellule de pointe de l'armée français affirme qu'il n'y aucun problème, de l'autre des sociétés éditrices d'antivirus demandent que soit enterré ce code à tout jamais

détruire le Web en quelques minutes

Althès coopère donc et décide d'effacer toutes traces du virus et divise le code en deux parties placées dans un coffre à la banque. Après enquête de la rédaction de Zataz, nous avons appris que la NSA, les services secrets américains, sont entrés en contact avec la société Althès lors du salon de la sécurité informatique qui s'est tenu au CNIT fin 2001. Faut-il avoir peur de Bad Track ? Oui, le code existe toujours et peut être activé à tout moment. Paradoxe de toute l'histoire, le secret qu'entoure Bad tracks, empêche même de réparer les failles qu'il exploite.
Une fois de plus, Zataz Magazine vous aura prévenu !

La réponse des éditeurs d'antivirus

Nous avons posé quelques questions aux Ingénieurs de Panda Software et de Network Associates à propos de ces virii qui sommeillent sur le réseau des réseaux et surtout nous leur avons demandé que faire en cas d'une rencontre de ce type. Voici leurs réponses.

Que faire si l'on découvre un virus ou un procédé viral ?
Il y a trois manières différentes de détecter les virus: la détection classique des signatures de virus, efficace pour la plupart des virus. Cette méthode n'est cependant pas valide dans certains cas, principalement ceux de virus cryptés. De nos jours, la manière de détecter les virus est très similaire dans tous les programmes d'éradication. Si tel antivirus laisse échapper un virus dans le système heuristique, il le détectera demain dans le système des signatures, et si ce virus peut déjouer cet antivirus, demain il ne le pourra plus.

Mais le mot " demain " signifie parfois très, très longtemps lorsqu'il s'agit de virus. La pièce maîtresse de la sécurité antivirus est la rapidité, non pas en détectant des milliers de virus, mais la capacité du fournisseur d'antivirus à offrir au client une solution rapide pour de nouveaux virus. Seules les entreprises avec un canevas de travail comprenant un service 24 heures sur 24 et 365 jours sur 365 sont à-même d'offrir une bonne solution.

Avez-vous déjà entendu parlé de Bad Track ?
Panda Antivirus : Non. Nos laboratoires ne semblent pas avoir eu en main ce code viral.

Network Associates : Nous trouvons dans nos bases internes un Cheval de Troie nommé "Bad track". Celui ci ne s'attaquerait qu'aux disques MFM. Nous n'avons pas plus d'information sur la date de création de cette détection. Coté éradication, elle est simple : on efface le fichier. Par contre pour le cas où ce Trojan aurait écrasé des secteurs physiques du disque, il n'y a pas de solution de récupération par un anti-virus. Pour ce qui est de «votre» Bad Track, personne, dans nos laboratoires n'en a entendu parlé.

Avis d'expert

Nous avons souhaité en savoir plus sur *Bad Track* qui commence à inquiéter l'élite de la sécurité informatique.
Nicolas Sadirac, le directeur de l'Epitech, département l'école Informatique Epita nous répond.

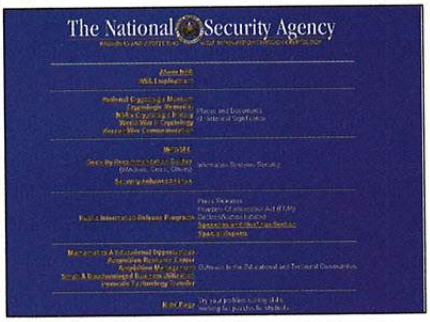
Existe-t-il aujourd'hui des virii qui sommeillent ?
Oui, obligatoirement. Il existe des moyens et des codes qui sont prêts à frapper. Il faut savoir qu'un code travaillé et étudié pour une cible précise est quasiment indétectable. Fait sur mesure, il contaminera dans la majorité des cas. Ce type de virus est très souvent utilisé dans des audits de sécurité informatique d'ailleurs !

Qui peut fabriquer ce genre de chose ?
Il est évident qu'ici nous avons à faire à des professionnels qui sont dans ce milieu depuis longtemps pour être passés maîtres de ce genre de programme.

Ces «armes» sont-elles à prendre aux sérieux ?
Oui ! Pour preuve nous allons proposer des cours, l'année prochaine, dédiés aux antivirus et aux virii.

Focus

Les acteurs de la cyberguerre



Tout action anthropique est soumise à ce que l'on appelle la loi de Murphy. Aini, tout élément contenu dans un système clos arrivera systématiquement à se déteriorer et finir dans un état de désordre. Le Web ne déroge pas à la règle. Toute information qui y transite se verra au bout du compte manipulée, transformée, voire détruite. Qui sont les auteurs de ces transformations ? Ceux pour qui justement l'information est synonyme de pouvoir : les services secrets, les pirates et les groupes autonomes. Qui sont-ils, quels intérêts portent-ils à contrôler, voir à transformer l'information ? Bienvenue dans la Cyberguerre.

L'information ? Elle a aujourd'hui plus de valeur que les armes. Les Etats-Unis consacrent aujourd'hui plus d'argent à ses services de renseignements informatiques qu'à ses corps d'armée, et l'Europe semble partie pour en faire autant. Cette guerre de l'information a un enjeu énorme : qui la contrôle, a en théorie une fenêtre sur les évènements à se produire. Et depuis ce tragique jour du 11 Septembre, cette équation n'a que plus de crédibilité.

Les bons, les brutes et les truands

On peut classer en trois catégories les acteurs de cette guerre de l'ombre : Les agents de services secrets, les organismes indépendants ou semi-autonomes incluant des associations de malfaiteurs telles que des groupes terroristes ou des groupes radicaux, les trafiquants de drogues, et les mafias. On termine par les particuliers tels que des pirates, ou des scripts kiddies. Ces individus peuvent parfois collaborer ensembles mais ils agissent généralement seuls en utilisant des outils particulièrement sophistiqués, virus, trojan, sniffer, pour rassembler, détruire ou exploiter des informations. Les intrusions illégales dans les ordinateurs peuvent également être classées par catégories :

Les attaques étrangères qui incluent des services d'intelligence, les terroristes, les groupes criminels, les concurrents économiques et les vandales. Les Etats- Unis ont d'ailleurs déjà eu affaire à ce problème en 1998. Un groupe baptisé "Master of downloading" avait piraté le réseau américain du Defense Information Systems Network qui contrôle des satellites militaires. Ils ont même réussi à récupérer des logiciels connus sous le nom de DEM, utilisés pour localiser des frappes de missiles et guider les troupes armées au sol. Dans une autre catégorie, les attaques d'initiés. Ici, l'intrus parvient par un accès légitime au système informatique et réalise des actions malveillantes pour gagner des privilèges non autorisés. Cette catégorie est la plus médiatique car finalement la plus visible, tel le piratage du forum du G8, où les coordonnées banquaires d'entre autres Bill Clinton et Bill Gates ont été volées.

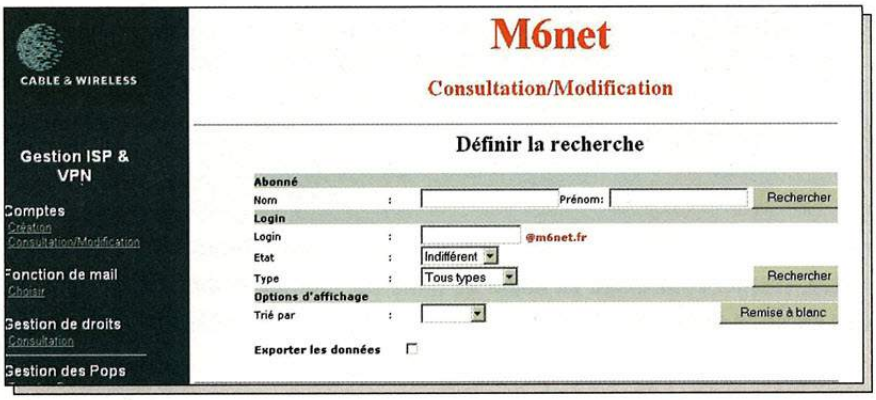
Espions et systèmes d'informations

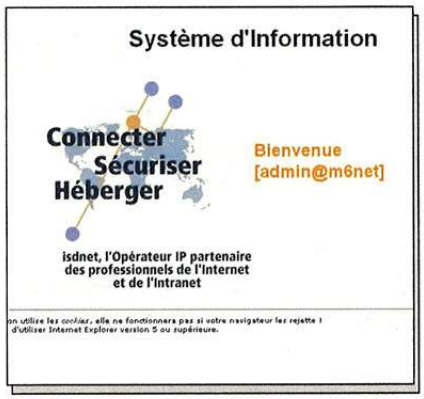
Les services d'intelligence étrangers se sont rendus compte que de nombreuses informations sensibles étaient disponibles sur le réseau. En utilisant des techniques d'extraction de données, un service d'intelligence étranger peut facilement extirper des données de centaines d'endroits disparates et combiner toute les informations acquises pour se fournir en éléments essentiels sur une nouvelle technologie.

Ce mode d'espionnage peut aussi, par exemple, rassembler des informations sensibles dans le cadre de recrutements ou de chantage. Le système DCS1000, ex Carnivore, mis en œuvre par le FBI, permet ainsi de traquer n'importe quelle information circulant sur des serveurs d'un fournisseur d'accès Internet complice. Deux versions issues du DCS1000 ont déjà été mises sur le marché : NetWitness Collector, de Forensics Explorers et Altivore de Network Ice. Le premier de ces outils capture les informations des réseaux locaux et réorganise en un tout permettant l'analyse des contenus. Le second offre une surveillance électronique sur mesure. Les vulnérabilités, sont aussi une information recherchée. Elles peuvent être exploitées dans un conflit. Exploiter, dégrader, interdire ou prendre le contrôle de l'information critique nécessaire pour répondre à une crise. Généralement désignées sous le nom de "guerres de l'information", ces attaques sur Internet offrent un avantage indéniable : la possibilité de rester anonyme. Les nations étrangères développent des programmes de guerre de l'information surtout contre les USA, car l'énorme confiance qu'accorde ce pays aux nouvelles technologies pour commander leurs infrastructures gouvernementales et privées est devenue leurs talon d'Achille. La plus grande menace du point de vue des informations confidentielles provient de la dérégulation des secteurs privés. Les USA l'ont compris en créant des fonds spéciaux, via des sociétés de capital risque nommées in-Q-it soutenues par la CIA. Elle détecte les sociétés privées développant des technologies de pointe, devient actionnaire et contrôle alors sa nouvelle acquisition. Un exemple, l'entrée récente dans le capital de Safeweb qui offre des technologies de protection de la vie privée sur internet. La technologie développée par cette entreprise rend impossible l'identification de la source. Officiellement, les espions américains s'en servent pour protéger leurs réseaux de communication. Officieusement, utilisée à grande échelle, elle permettrait de mener une attaque informatique ciblée contre des serveurs étrangers.

M6Net sauvé par un hacker

Imaginez qu'il soit possible d'avoir accès à la base de données des clients du fournisseur d'accès M6net, d'effacer tous les comptes ou même d'en créer. Bref, mettre sur le carreau un FAI de plus de 400.000 abonnés. ZATAZ Magazine vous raconte en exclusivité une histoire qui serait restée secrête sans notre indiscretion.





C'est par un beau jour de février qu'un hacker blanc, que nous appelerons Mr. X, nous contacte et nous annonce avoir accès à la base de données clients de M6net. Il n'a copié aucune donnée, juste découvert comment il était possible d'avoir accès à tous les outils d'administration du FAI M6net. Il a en effet réussi, par des moyens que nous devons garder secrets, à trouver le mot de passe de l'administrateur. Avec cette trouvaille, n'importe qui aurait pû créer, effacer ou surveiller les comptes des abonnés de m6net.

Je ne suis pas un pirate

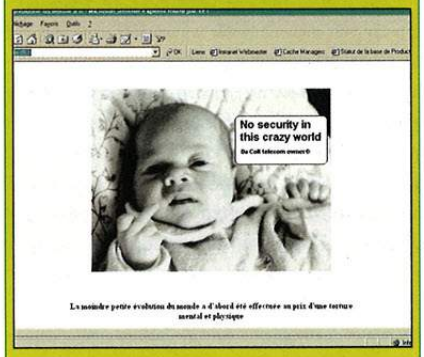
Zataz Magazine a donc immédiatement contacté cette société par le biais de son e-mail, info@m6net ainsi que par son numéro de téléphone public, un "08" à 0.38 euros la minute. Au bout de deux appels, nous avons heureusement eu une très bonne réaction d'un des responsables informatique, drôlement inquiet, qui a pu mettre en œuvre, quasiment dans l'heure, toute la procédure de sécurisation. Inutile d'insister sur le fait que nous avons croulé sous les remerciements. Les dégâts que cette faille étaient facilement chiffrables à plusieurs millions de francs, de quoi faire fermer sans recours toute l'activité Internet de M6.

M6, une cible de choix

Alors que M6 lançait la première édition de Loft Story, les internautes se sont investis d'une passion sans précédent pour les rondeurs de Loana et les trépidantes histoires de ses compagnons (qui a peté ?).

On ne comptait plus les sites parodiques et pirates de Loft Story, certains proposant de regarder les lofteurs sans être obligé de passer par les pages imposées par M6. Des logiciels, créés à la va-vite, mais d'une efficacité redoutable, parvenaient même à capter les flux vidéos de chaque caméra pour les retransmettre sur les écrans des internautes, le tout sans publicité ni restriction commerciale quelconque. D'autres programmes, plus évolués, diffusaient simultanément deux caméras sur le même écran. Autant dire qu'Akamaï, le prestataire vidéo de M6, s'est vite fait supplanter par quelques programmeurs en herbe de talents ! L'autre problème qu'a rencontré M6 a été l'énorme quantité de pages piratées du site Loft Story. Un hacker, signant Mr Tordu piratera plusieurs fois le site de Loft Story pour exprimer son mécontentement sur la perversité de l'émission. Un délire numérique qui a d'ailleurs des chances de se renouveler avec l'arrivée sur nos petits écrans de Loft Story 2. " Mais nous y travaillons " tente de nous rassurer le responsable informatique que nous avons pu joindre chez M6.

TF6 piraté



Le site web de la chaîne satellite TF6, alliance de TF1 et M6 pour le bouquet satellite TPS, aura elle aussi connu les affres d'un piratage. Le visiteur, qui a signé *Da Colt Telecom*, n'y a pas été de main morte (voir capture d'écran). Son message placé sur la page de garde de TF6 est sans équivoque : "La moindre petite évolution du monde a d'abord été effectuée au prix d'une torture mentale et physique". Serait-ce là un message d'un disciple de Mao ?

www.tf6.fr

Piratage de Films

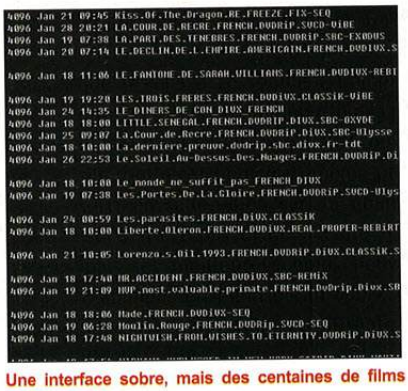
Les vrais réseaux clandestins

On parle de plus en plus de copies de films sur internet. Tous sont tous unanimes. Walt Disney, News Corp, Miramax, Twentieth Century Fox, Paramount, Universal, Warner l'affirment. La copie de films sur Internet commence à devenir critique. Il faut agir ! ZATAZ Magazine vous entraîne dans les méandres de ce réseau qui font trembler les Majors.

Ce n'est pas du cinéma

Le piratage de films vidéo en format DivX sur Internet fait aujourd'hui autant fureur que le MP3 à ses débuts. Comprenez les internautes, ils ont aujourd'hui la possiblité de télécharger en une heure ou deux un film qui n'est peut-être même pas encore sorti en salle. Bien sûr, la qualité de la vidéo n'est pas égale à celle d'un DVD, mais les meilleures copies peuvent être visionnées en plein écran 800 x 600 dans une qualité plus que satisafisante. Le coût d'achat d'une copie vidéo : Zéro. Seul le temps de téléchargement est à prendre en compte. Devant le succès écrasant de la copie de films, de vastes réseaux de pirates se sont organisés. Nous parlons bien de réseaux car ceux-ci sont extrêmement bien organisés et chaque membre a ici une spécialité, allant de l'encodage du film en DivX, jusqu'à l'employé d'une Major qui donnera discrètement une copie master d'un film avant même sa sortie en en salles.

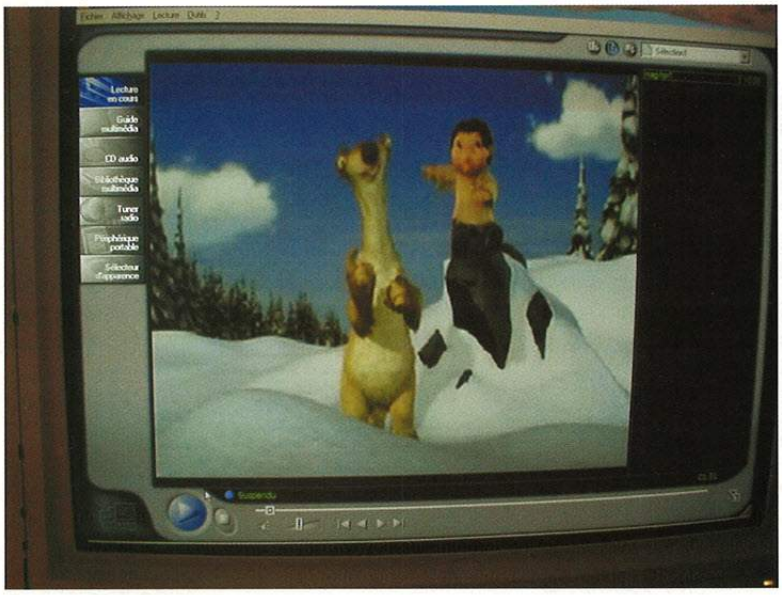
Si le risque est grand pour ces pirates (de fortes amendes, voire la prison), les réseaux underground liés à la copie de films sont loin d'être inquiétés par les annonces des Majors. «Ca nous fait même bien rire» nous explique X, membre d'un des plus importants groupes américains sur ce marché. Car il faut bien parler de marché de la copie pirate de film. Les groupes se font même une guerre sans merci, pour la renommée bien sûr. C'est à celui qui sortira le premier LA nouveauté, le gros Hit. . Un exemple, la copie du film «Monsters» de Walt Disney, sorti en mars 2002, était déjà diffusée sur les serveurs FTP pirates en novembre 2001.



Une interface sobre, mais des centaines de films disponibles !

Un autre exemple de serveur fournissant des films pirates. Toutes les dernières nouveautés sont là !

Les sources des pirates restent dans la majorité des cas secret-défense. «Il n'est pas rare de voir des copies d'un film arriver sur les boards (serveurs FTP) avant même que les publicités envahissent les panneaux d'affichage et magazines» nous expliquera un collectionneur de copies. L'exemple en date est celui du film Vidocq, distribué en Divx et de qualité irréprochable, proposé sur le web en janvier 2002, alors que sa sortie officielle en DVD date de début mars. Les exemples de



A peine sortis au cinéma, des nouveautés comme Ice Age sont envoyés sur Internet en format DivX. Le circuit est bien rôdé. On se demande ce que font les autorités !

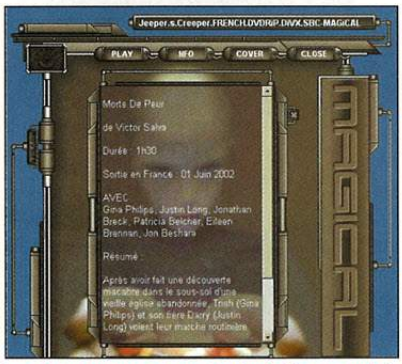
ces films qui sortent en avant-première sur le web sont nombreux. Plus le film est attendu dans les salles, plus ce dernier sera rapidement mis sur les boards pirates. Il suffit de lire les forums dédiés à ce genre de contrefaçon pour être étonné de la réactivité des groupes copieurs. Pas question, non plus, de parler de films de mauvaise qualité, interceptés à la sauvette avec le camescope de papa dans la salle de cinéma du quartier. Nous avons pu visionner des copies de film comme *Ocean Eleven*, *Le baiser mortel du dragon*, ou *Les Autres* en plein écran, avec une qualité de vidéo proche du DVD.

Cinéma Paradisio !

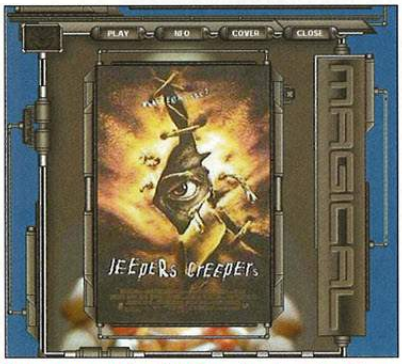
Les groupes de «pirates» de film mettent même un certain point d'honneur à diffuser des copies de qualité, sans parler des petits à côté qui peuvent faire monter leurs cotes de popularité. Chaque copie est suivie d'un fichier texte, appelé plus communément «lisezmoi.nfo». Dans ce document vous y trouvez le nom du groupe, la date de réalisation de la copie, le support, la présence d'éventuels sous titrages, etc... Certains pirates poussent même leur *professionnalisme* à proposer des copies dotées de plusieurs pistes audio qui pourront être choisies selon la langue du film souhaitée, (avec un lecteur compatible multilangues comme Bsplayer par exemple). Sans parler de groupe, comme *Magic*, qui n'hésite pas à mettre une bande annonce musicale de ses prochaines réalisations avant le film copié. Le «Prochainement sur un ftp près de chez vous» a fait beaucoup d'effets sur les amateurs de DivX" nous explique un internaute féru de films. Le groupe *Magic*, pour vanter sa force et son efficacité, avait apposé cette phrase dans l'introduction d'une copie pour promouvoir la sortie en copie du film *Ice Age*. D'autres groupes proposent carrément un petit logiciel qui diffuse le film, mais aussi imprime la jaquette, donne des infos sur les acteurs, le synopsis et tout ceci en musique ! On peut estimer qu'aujourd'hui il existe une centaine de groupes importants dans le monde dédiés à ce genre de contrefaçon. Les plus connus sont MAGIC, SNOW BOARD, ULYSSE, DOMINION, ESOTERIC, EVILSO, VIBE, SBC, CLASSIK, REBIRTH, EDEN. Côté production, on peut estimer aujourd'hui que tous les films qui finissent sur grand écran, rejoignent aussi, un jour ou l'autre, les boards pirates. Une étude récente, commandée par les Majors, effectuée par une agence de détective, annonce plusieurs millions de téléchargements par jour, ils sont loin du compte.

Les outils du pirate de film

Avant de pouvoir copier le film, il faut déjà avoir une source qui va permettre de copier le film original. Nous vous expliquons ceci dans notre encadré "Différentes formes de copie". Une fois le film "master" en main, le pirate va le réduire en taille afin que ce dernier puisse être diffusé sur internet. Pour ce faire il va disposer d'une multitude d'outils qui vont lui permettre cette réduction. On ne présente plus DeCSS qui permet de réduire un film DVD afin que ce dernier puisse tenir sur un simple CDROM de 700 Mo. Le pirate va ensuite le réduire encore, afin que sa diffusion puisse se faire de manière encore plus simple et rapide. Il va pour cela utiliser des logiciels comme IsoBuster qui vont lui permettre de créer une image du film en " .bin ", exemple zataz.bin. Une fois copié, ce fichier ".bin" avec des logiciels comme Cdrwin ou encore Fireburner, le pirate va pouvoir lire sa production sur des lecteurs comme Powerdvd. Le comptage avec un logiciel de type Winrar finira de diviser le film en plusieurs dizaines de morceaux, plus facilement diffusable sur le web.



Les pirates proposent aussi un logiciel pour accéder aux informations et bonus des films.



Vous pouvez même imprimer les jaquettes de vos films préferés !

GLOSSAIRE

.bin/.cue : Format d'image de CD.
Iso : Clone parfait d'un CD.
Release : Réalisation d'un groupe pirate.
Master : Original ou la première copie avant duplication.
Rip : Vient du mot ripper, enlever. On parlait déjà de ripper un jeu dans les années 80. Enlever une musique, un dessin, ...
FTP / Board : File Transfert Protocol. Espace de stockage.

Cyber agent contre pirates de film

Les studios de cinéma tentent désespérément d'éviter le désastre du peer to peer, l'échange d'internaute à internaute avec des outils de type Napster, Gnutella, Morpheus, ... qui a frappé l'industrie de la production musicale. La chasse aux pirates de films numérisés a entraîné l'éclosion de cyber-agences de détectives comme Vidius, une entreprise de Los Angeles dont le chiffre d'affaires a progressé de 350% au cours de l'année 2001. Cette agence annonce un chiffre de 4 millions de fichiers de films numérisés qui sont échangés chaque jour, contre 550 000 il y a deux ans. L'étude ne se base que sur les échanges via les outils peer to peer. (Source : Chicago Tribune via l'ADIT).

C'est arrivé près de chez vous

Les pirates diffusent leurs copies de différentes manières et sous différentes formes. La plus connue est directement via un site web. Le pirate y dépose son film et il ne reste plus qu'à télécharger. Les fournisseurs d'espaces gratuits comme Free, Multimania font la traque et n'hésitent plus aujourd'hui à effacer les comptes douteux. Certains pirates ont trouvé une série de parades qui permettent une diffusion via site web plus efficace. Pour cela l'utilisation de logiciel comme BOBDown qui permet de retrouver un film caché dans les méandres du web. A la condition où ce dernier a été chiffré en " .bob ". Le logiciel se chargera de vous rapatrier le film, à un débit souvent très lent. Dans les autres modes de diffusion, nous allons voir maintenant le plus rapide et surtout le plus efficace avec l'utilisation de FTP. Les groupes de pirates disposent de plusieurs comptes leur permettant de placer leurs copies. Dans la grande majorité des cas les espaces sont "empruntés" à des serveurs web d'entreprises. Les groupes y déposent leurs films et la distribution peut commencer. Une diffusion souvent de serveur à serveur. Des outils comme FXP permettent de transférer en toute transparence des dizaines de films en une seule journée. Certains autres outils réduisent les fichiers de manière à être difficilement compréhensibles par les non initiés. Le programme est nommé en «.bin» et reste illisible. Un logiciel nommé Isobuster décortiquera le film de manière à le rendre lisible par tous. La grande majorité des films diffusaient sur le web le sont sous le format «.rar» un format de compression qui permet de réduire un film en une cinquantaine de fichiers séparés.

La dernière séance ?

Les "Majors" commencent donc à réagir face à ce piratage. Il est cependant apparu dans notre enquête que certains salariés de ces Majors participaient à ces

Photo : Dreamworks

Les différentes formes de copies

La scène "pirate" dédiée au film se divise en sous réseau. Chaque ramification ayant sa propre spécialisation. Voici les différentes formes et chemins que peuvent prendre, aujourd'hui, les copies de film.

Le dvd rip : Par rip, comprenez Ripper, enlever. Le DVD rip est le clone du film provenant d'un DVD.
Le camcord : La plus vielle et la plus "underground" des méthodes de pirate de film. Ici le "pirate" va prendre sa caméra, un pied, des batteries et va filmer le film directement dans la salle.
Le finger print : Le plus recherché car ce dernier n'est rien d'autre que le piratage du film directement via le studio de production. Le finger print possède le plus souvent un "Time counter", un compteur servant à la production pour monter le film. Il n'est donc pas rare de trouver sur certains ftp pirate le même finger print mais pas toujours avec le même montage. Les collectionneurs se les arrachent.
Le press finger print : Ce dernier moyen de copier le film provient directement de certains journalistes spécialisés. Ces journalistes reçoivent la cassette du film afin de pouvoir en faire une critique avant sa sortie en salle. Il suffit que cette cassette traîne dans un coin et le tour est joué.

réseaux parallèles en diffusant certaines productions. Pourquoi ? Une nouvelle forme de Marketing ? Nous en doutons. Les majors vont en tout cas avoir du mal à surveiller chaque salle de cinéma, chaque société qui s'occupent des DVD commerciaux, chaque attaché de presse et journaliste ayant en main les masters.
Attaquer les créateurs des outils de compression comme DeCSS, tenter de freiner certains réseaux comme le groupe Drink or Die arrêté en décembre 2001, cela peut-il suffire ? Nous pouvons en douter aux vues de la diffusion pirate qui s'effectue aujourd'hui sur le web.

Une recherche sur le groupe de pirates Magic permet de trouver en quelques minutes une flopée de films...

Une liste de sites pirates fournie par Google.

Que dit la loi ?

Que dit la loi au sujet de la copie de film ? Nous avons posé la question à Maître Murielle Cahen, spécialiste multimédia. Les films, appelés vidéogrammes par le code de la propriété intellectuelle sont protégés par le droit d'auteur par les articles L112-1 et L112-2 qui mentionne explicitement :
«Les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images, sonorisées ou non, dénommées ensemble œuvres audiovisuelles». Par conséquent les films sont soumis à l'article L122-4 qui dispose «Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque». Par conséquent la copie de film est une contrefaçon punie de deux ans d'emprisonnement et 152.449 Euros (Soit 1.000.000 de Francs) d'amende selon l'article L335-4.

La copie privée est autorisée mais cependant dans le cas du vidéogramme soumise à un régime particulier qui impose la rémunération pour copie privée des ayants droits.
Pas question donc de copie de sauvegarde et encore moins question de mise à disposition sur Internet.

«Financièrement ca peut rapporter si la nouveauté en vaut la peine»

Max, un pseudo, gravite autour de la contrefaçon de films depuis le début des années 90. Un collectionneur qui est très vite devenu un fournisseur de Master de DVD. Et pour cause, il travaille dans une société de Singapour qui produit des DVD commerciaux.

Max, tu es un français expatrié, comment es-tu venu à la copie de film ?
Très simplement. Je travaille dans un milieu proche de la production de DVD commerciaux et avant d'être à Singapour je suis passé par Hong Kong et les Philippines. Là bas les films sortent rapidement, donc facile de s'en procurer pour quelques dollars.

Une fois récupéré que fais-tu de ces films ?
Je les envoie à mes correspondants qui font la modification et la diffusion.

Ca te coûte l'achat de ces DVD, mais est ce que cela te rapporte quelque chose ?
Financièrement ca peut rapporter si la nouveauté en vaut la peine, sinon c'est l'échange qui me rapporte le plus. Le fait de côtoyer des groupes importants me permet aussi d'avoir des news avant tout le monde.

Tu te fournis où ?
Je resterai discret sur ce sujet. Mais il suffit de se promener dans certaines boutiques pour déjà trouver quelques grosses nouveautés DVD. La numérisation avec ReplayTV 4000, de SONICblue, permet d'enregistrer et de transférer ensuite le film sur le réseau.

As-tu peur du gendarme ?
Honnêtement oui mais si je sais qu'il y a peu de chance d'être pris la main dans le sac. J'ai surtout peur de la douane qui peut saisir les DVD que j'envoie par voie postale.

Chaos Computer Club France

Le chasseur de pirates

Jean-Bernard Condat

Au début des années 90, un jeune étudiant lyonnais, Jean-Bernard Condat, créé avec un membre de la D.S.T. un club de hackers baptisé Chaos Computer Club France. Son objectif : identifier et éliminer les pirates qui s'introduisent dans les serveurs de grosses entreprises françaises. A peine quelques mois après sa création, le résultat ne se fait pas attendre : une vague d'arrestations éradique l'Underground français. 10 ans après les faits, Jean-Bernard Condat se confie à Zataz Magazine, et surtout s'explique.

Vous avez créé un club, le Chaos Computer Club France, pour faire arrêter bon nombre de pirates informatiques. Les services de contre-espionnages français ont grandement profité de vos informations pour lancer des arrestations. Pourquoi un tel club ?

A la demande de mon officier traitant Jean-Luc Delacour (NDLR : son contact à la D.S.T.), j'ai accepté de mettre en place un confessionnal pour pirates naissants ainsi que pour chefs d'entreprise en manque de confessions sécuritaires. Nous l'avons baptisé Chaos Computer Club France. Le but étant de ficher tout intervenant à des fins de recensement.

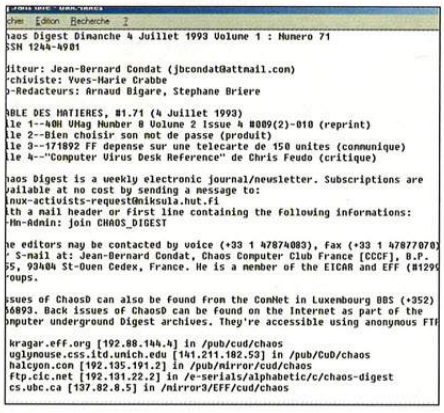
Vous étiez un hacker, partie intégrante du phénomène undeground des années 90. Qu'est ce que cela représente pour vous ?

L'underground reste l'usage de documents publics dans un but de découverte de champs d'application non classiques. L'effet de nouveauté est un des principaux moteurs de nos amis flibustiers, la réalité d'une possibilité d'arnaque le piment de leur motivation. Prenez un interdit, affichez-le en gros et vous obtiendrez une cause de piratage.

Les pirates et les hackers ont-ils évolué, depuis l'époque du CCCF ?

Un pirate était auparavant un as de la duplication de jeux Atari ou de disquette 5' 1/4. Ensuite, nous avons vu apppraître les fouineurs de logs sur les consoles Unix des salons informatiques, les voleurs de «white papers» des constructeurs de modems. Enfin, nous apercevons les phreakers (pirates téléphoniques) lecteurs assidus de forums comme 2600 ! Rien de bien époustouflant que l'étude d'une sous-population composée d'adolescents généralement de parents divorcés ou non attentifs à leurs progénitures et en quête d'exploits sporadiquement nationaux.

Le pirate est celui qui transcende l'usage des nouvelles technologies au quotidien. C'est rare de voir un adolescent faire plus que de comprendre le manuel de son lecteur TPS ou d'acheter chez Surcouf un graveur pour immortaliser quelques heures de Napster. Sans intérêt et sans survie. Il faut trouver autre chose pour que cette race de joyeux drilles trouve encore la substance de leur action.



```
Chaos Digest Dimanche 4 Juillet 1993 Volume 1 : Numero 71
ISSN 1244-4901

Editeur: Jean-Bernard Condat (jbcondat@attmail.com)
Archiviste: Yves-Marie Crabbe
Co-Redacteurs: Arnaud Bigare, Stephane Briere

TABLE DES MATIERES, #1.71 (4 Juillet 1993)
File 1--NOH VMag Number 8 Volume 2 Issue 4 M009(2)-010 (reprint)
File 2--Bien choisir son mot de passe (produit)
File 3--171892 FF depense sur une telecarte de 150 unites (communique)
File 4--"Computer Virus Desk Reference" de Chris Feudo (critique)

Chaos Digest is a weekly electronic journal/newsletter. Subscriptions are
available at no cost by sending a message to:
linux-activists-request@niksula.hut.fi
with a mail header or first line containing the following informations:
X-Mn-Admin: join CHAOS_DIGEST

The editors may be contacted by voice (+33 1 47074083), fax (+33 1 47077070)
or S-mail at: Jean-Bernard Condat, Chaos Computer Club France [CCCF], B.P.
55, 93404 St-Ouen Cedex, France. He is a member of the EICAR and EFF (#1299
groups.

Issues of ChaosD can also be found from the ConNet in Luxembourg BBS (+352)
46893. Back issues of ChaosD can be found on the Internet as part of the
computer underground Digest archives. They're accessible using anonymous FTP

kragar.eff.org [192.88.144.4] in /pub/cud/chaos
uglymouse.css.itd.unich.edu [141.211.182.53] in /pub/CuD/chaos
halcyon.com [192.135.191.2] in /pub/mirror/cud/chaos
ftp.cic.net [192.131.22.2] in /e-serials/alphabetic/c/chaos-digest
cs.ubc.ca [137.82.8.5] in /mirror3/EFF/cud/chaos
```

Pour vous quels sont les ennemis aujourd'hui sur le web ?
Le Web est un des outils de l'IP v4. J'attendrai l'IP v6 avant de vous répondre. Je n'ai guère de chance de le faire avant quelques mois.
L'ennemi du Web reste le magma de chiures informationnelles sans intérêt que tout un chacun se croit en droit de mettre en devanture de son site. www.condat.nom.fr ne sera jamais autre chose qu'une bibliothèque morte. Surtout que je m'inquiète de plus en plus du devenir de mes écrits électroniques et de ces déjections.

L'avis du contre espionnage français

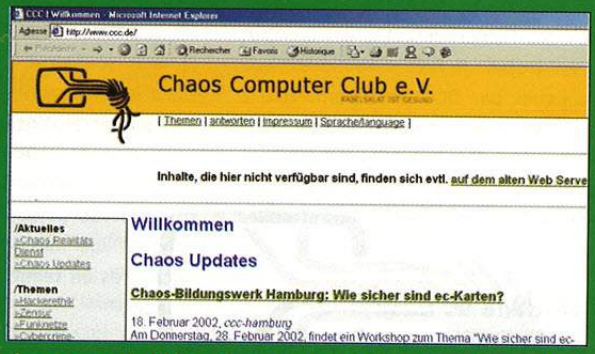
Nous avons posé quelques questions au sujet de ce club au responsable de la section patrimoine de la Direction de la Surveillance du Territoire (DST).

Parlons un peu de l'histoire du Chaos Computer Club et de sa passerelle française ? La D.S.T. avait-t-elle vraiment infiltré ce club ?
A partir du moment où on s'intéresse à ce qui se passe dans ces milieux là, on diligente des enquêtes tant en France que sur le plan international dans la mesure ou Internet aboli les frontières. Nous avions une enquête en cours sur des affaires d'intrusions sur notre territoire qui nous a amené à identifier des auteurs qui se situaient en Allemagne. L'enquête au sujet de certains membres notamment du Chaos Computer Club allemand, a montré qu'ils ont voulu vendre des informations aux services secrets soviétiques (K.G.B.). Nous nous devions d'être présents pour stopper ce genre d'agissements.

Aujourd'hui, peut-il y avoir encore de l'ingérence étrangère dans des petits clubs informatiques ?
Le rôle de notre direction est de s'intéresser au milieu, dit, de hackers. Encore faut-il être prudent avec le terme hacker. Il faut s'intéresser à des gens qui ont des idées ainsi que d'éventuelles intentions malveillantes pour les infrastructures françaises. Il faut savoir raison garder, analyser les choses, il faut les étudier tranquillement. Mais nous veillons !

Tout a commencé en Allemagne

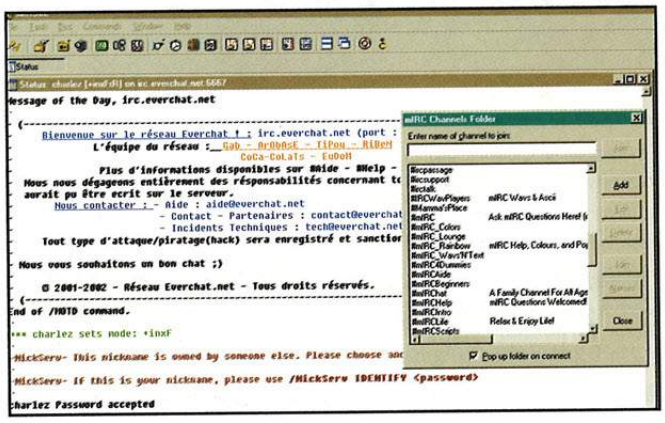
Le groupe de «hackers» du Chaos Computer Club, le club allemand d'origine, est quant à lui né en 1984 (date mythique!). Des passionnés d'informatiques qui veulent que soit libérées les connaissances numériques. Voici leur manifeste : «Nous réclamons la reconnaissance d'un nouveau droit de l'homme, le droit de la communication libre, sans entrave, à travers le monde entier, entre tous les hommes et tous les êtres doués d'intelligence, sans exception. Les ordinateurs sont des instruments de jeu, de travail et de pensée. Mais ils sont surtout le plus important des nouveaux médias. Nous nous élevons contre la politique de panique et de crétinisation qui sévit en matière d'ordinateurs, de même que contre les mesures de censure de groupements industriels internationaux, des monopoles des postes et gouvernements».
Le premier coup médiatique du C.C.C. date de 1984. Le groupe détournera 135.000 marks de la Caisse d'épargne de Hambourg. Une manière de montrer les failles du système.
Fin des années 80, le C.C.C. est devenu un groupe de référence fort de 500 membres, actifs et sympathisants. Une cible pour des services de renseignements étrangers, comme le KGB. Certains membres seront recrutés. Ils pirateront, entre autre, Thomson (ex Thalès), qui servira de passerelle entre les pirates et un agent russe basé en Australie. Les services secrets russes apparaissent aussi en France dans l'affaire du piratage

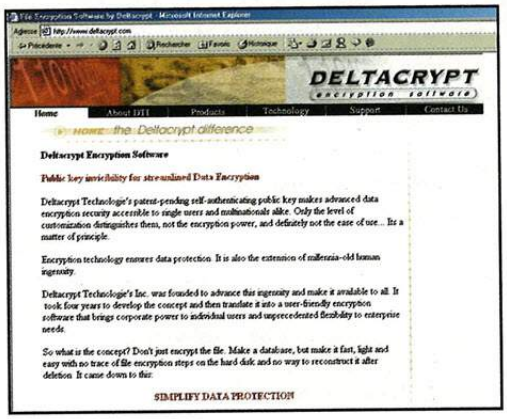


du serveur de Philips France en 1986 à Fontenay-sous-Bois. Philips travaille à cette époque avec les militaires sur un projet proche des missiles Exocet. Des informations seront volées et revendues aux russes.
En 1987, un juge français fait perquisitionner les locaux du Chaos Computer Club allemand. La police y découvrira que des membres du C.C.C. ont piraté le Centre à l'Energie Atomique français, le CNRS, l'Observatoire de Paris. En 1989, les services de contre-espionnages allemands, le BFV, arrête une dizaine de hackers qui travaillaient, depuis quatre ans déjà, pour le KGB. Le Chaos Computer Club France va naître de cette multitude de piratages sur le territoire français afin de regrouper des informations, tracer et remonter les acteurs criminels.

IRC : tout pour se protéger

L'IRC est l'un des outils les plus populaires du web. Et pour cause, on y trouve de tout. Du bon comme du mauvais. Voici les trucs à savoir pour éviter le pire. D'abord il vous est fortement conseillé d'installer un antivirus qui pourra être couplé avec un firewall. Sur le Net vous trouverez des firewalls gratuits, allez jeter un œil sur notre site dans la partie logiciels.





Vous désirez donc être présent sur les chats par le biais d'outils IRC. Il est judicieux de désactiver, en premier, le «DCC» comprenez l'option de réception de fichier afin que personne ne puisse vous envoyer des fichiers infectés par un virus et/ou un trojan. Il faut savoir aussi que communiquer par DCC peut permettre à un pirate de connaître votre adresse IP ce qui pourra lui laissera l'opportunité, à l'aide de pings, de vous faire déconnecter du serveur de chat, voire de vous attaquer à l'aide de logiciels de piratage.

Précautions de base

Vous pouvez configurer le DCC en cliquant sur l'option du même nom et cochez la ligne à chaque «ignore all».

- *On send request* > Evite un envoi de fichiers vérolés
- *On chat request* > Evite un message de personne à personne.

Pour la jouer un peu plus sécurisé, allez dans l'option *Use random local ports* qui peut se traduire par *Changer de port fréquemment*. Une option qui bloquera la grande majorité des script-kiddies. Il vous faut savoir que MIRC implante dans son programme un système *Identification Daemon* en abrégé *Identd* afin que les fournisseurs d'accès et autres serveurs puissent savoir qui vous êtes. Dans l'onglet *Identd* ne cochez pas *Show Ident Requests* afin de minimiser la révélation de votre identité...

Si vous souhaitez chiffrer vos conversations sur IRC sachez qu'il existe quelques logiciels et plugins gratuits qui vont vous permettre de causer en crypté. Le fonctionnement reste simple. Vous décidez d'un mot de passe avec votre correspondant et les messages ne pourront être déchiffrés en temps réel sans ce précieux sésame.

Restez anonymes !

Chater anonymement est possible mais il faut savoir que de plus en plus de serveurs limitent l'utilisation de proxies. Si vous avez l'autorisation d'en utiliser, voici comment procéder. Lancez votre logiciel de chat. Allez dans File>options puis Connect>Firewall, dans la boite de dialogue, cocher la case *Use Firewall* et dans *Protocol* choisissez *Proxy*. Dans *Hostname>UserID*, mettez le nom de votre Proxy et ne placez rien dans l'onglet Password. Choisissez le port 1080. Allez dans Local info, mettez dans Local Host l'adresse de votre Proxy et n'inscrivez rien dans la case *IP Adress*. Dans *On connect, always get*, décochez toutes les cases. Ensuite dans *Lookup method* choisissez *Server*.

Les adresses :

Logiciel IRC gratuits
http://www.epiknet.net
http://www.f-irc.com

Logiciel IRC payant
http://www.mirc.com

Logiciels de chiffrement IRC
http://www.deltacrypt.com
http://www.chez.com/ve2vdi/
http://www.tlsecurity.net/windows/filearchive/MircCrypt1.1.6.html

ICQ & messenger : chatez couverts

ICQ et Messenger sont deux logiciels formidables pour discuter entre internautes. Force est cependant d'admettre qu'ils peuvent aussi être assez dangereux si quelques précautions que nous vous détaillons ici ne sont pas prises....

ICQ est un logiciel connu et reconnu, surtout par les diverses failles qui ont émaillé son histoire. Déjà désactivons le mouchard installé dans ce programme. Pour cela allez dans :
Démarrer>Executer>Regedit> Hkey CurrentUser>Software>Mirabilis>Icq> DefaultPrefs>
Puis trouvez la clef «update» puis modifiez le «yes» en «no». Lorsque vous aurez éliminé la clef dans la base de registres dénommée : «active server list», vous serez débarrassé du mouchard d'ICQ.

Bannir automatiquement les messages inopportuns

- Cliquez sur l'icône «Sécurity & Privacy» dans le menu d'ICQ.
- Dans la fenêtre qui apparaîtra, choisissez l'onglet Words List
- Pour entrer de nouveaux mots vous devrez cliquer sur Add
- Que faire des messages contenant les mots listés : Soit remplacer ces fameux mots par autre chose, soit bloquer complètement ces messages.

Filtrer les contacts

Cliquez sur l'onglet «Ignore» dans cette même fenêtre de sécurité
- Dans la liste, vous pourrez indiquer les contacts indésirables

Interdire la publicité & les urls

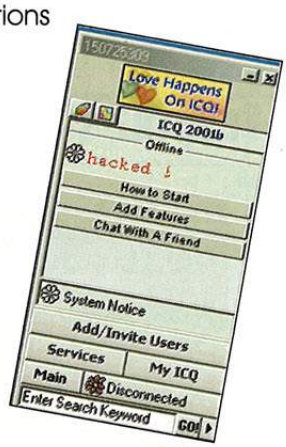
- Cliquez sur «Préférences» dans le menu ICQ
- Dans la partie gauche dans la nouvelle fenêtre, choisissez l'onglet Events
- Puis, sur la droite, choisir Web Page (URL)
- Cliquez sur la troisième option pour refuser automatiquement la réception d'URL.
- Vous pourrez de plus interdire dans la fenêtre Events plusieurs événements qui pourraient être incontrôlables.

Autres options

- Accepter uniquement les messages des gens de votre liste de contacts
- Ne pas accepter les message Multi-récipients
- Ne pas accepter les messages EmailExpress ou WWPager
- Ne pas autoriser la connexion avec des versions logicielles ICQ antérieures

Paramétrer les niveaux de sécurité

Pour éviter les attaques d'un utilisateur mal intentionné, cliquez sur la commande «Préférence & Sécurity» puis «Sécurity & Privacy». Cochez les onglets «Ignore List» et «Accept messages only from users on my contact list». Cachez partiellement votre adresse IP (Internet Protocol) en cochant



l'option «Do not publish IP Adress», «Do not accept WWPager Messages» et «Do not accept Email Express messages».
Important sélectionnez «Do not allow Direct Communication with previous Icq software versions». Cette fonction empêchera la communication avec d'anciennes versions d'ICQ. On vous invite à lire «ICQ» édité par Micro Application.

Les adresses :

Le logiciel ICQ
www.icq.com

Le logiciel Messenger
http://messenger.msn.fr

Le logiciel SIMP
http://www.secway.com/

Pour les utilisateurs de Messenger

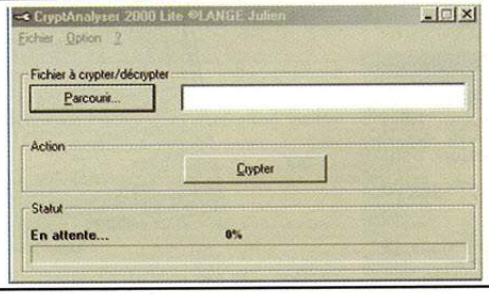
Messenger, plus connu sous son petit nom de MSN est un programme de Microsoft. Il est téléchargeable gratuitement par le biais de Windows Update. Un spywar, un espiongiciel est installé avec MSN. Eliminez-le en allant dans Démarrer>Executer et rentrez la commande «msconfig» puis dans l'onglet «Démarrage» décochez «Load QM.exe». Il existe un excellent outil pour causer en toute sécurité sous MSN. Le logiciel nommé SIMP, Secway Instant Messenger Privacy, va chiffrer vos messages qui ne pourront être lus qu'après un échange automatique de clé. Facile d'utilisation, puissant et français, il utilise un Proxy transparent, indépendant de MSN Messenger. Trois modes de fonctionnement sont possibles : Mode authentifié et chiffré (algorithmes RSA + Twofish) garantissant l'identité des correspondants. Mode chiffré (algorithmes DH + Twofish) et un mode normal, pour assurer une compatibilité totale avec vos interlocuteurs ne disposant pas de Simp.

Appz!

Voici notre sélection de programmes à télécharger. Tous vont rendront de grands services alors n'hésitez pas une seconde à vous les procurer !

Cryptez tous vos textes ou programmes

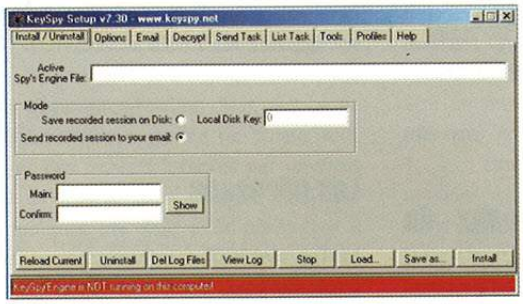
Nom : Crypto-analyser Langage : FR Poids : 0,04 mo License : Freeware



Ce logiciel de chiffrement va vous permettre de crypter tous ce qui va vous passer sous la main : textes, programmes, fichiers zip. Le programme crypte vos données à l'aide du clé de 128 bits. A noter qu'enfin que ce logiciel, créé par Julien Lange, peut se transporter via une simple disquette. Pratique pour pouvoir décrypter vos données sensibles à tout moment chez n'importe qui.

Surveillez votre PC en votre absence

Nom : Key Spy // US | 0,41 mo | Shareware



KeySpy 6.5 enregistre toutes les frappes qui seront effectuées via votre clavier informatique. Cet espion chiffre les informations et peut vous les envoyer par e-mail durant votre absence. Outil parfait pour savoir qui a fait quoi sur votre machine.

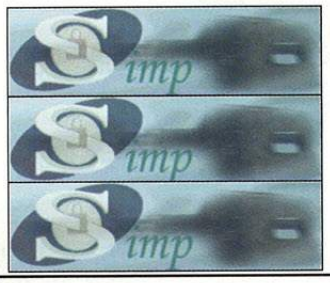
Surfez anonymement en tout sécurité avec le navigateur Zataz !

Nom : Nis-ZATAZ // FR | 8,00 mo | Shareware

Le navigateur sécurisé de ZATAZ Magazine va vous permettre de surfer en toute tranquillité. Choix du proxy, scan de vos ports PC, surf anonyme, traceur, sans parler des 150 autres options vous permettant un surf optimal et efficace.

Chiffrez vos conversations sur MSN Messenger

Nom : Simp Langage : FR Poids : 0,80 mo License : Freeware

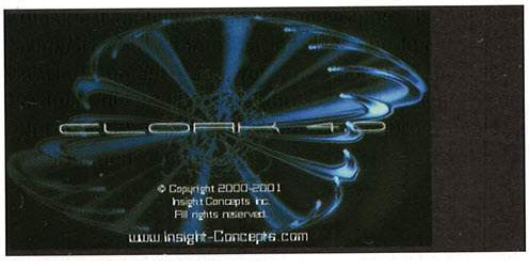


MSN Messenger est un outil facile d'accès, convivial. Il nous ferait presque oublier la sécurité. Grégoire Sirou, ingénieur pour la société Secway - secway.com - et développeur du logiciel Simp propose de protéger vos conversations de manière simple et ultra efficace. Les conversations de Messenger circulent en clair vers les serveurs Internet de Microsoft ! Un pirate, ou même Microsoft, peut ainsi intercepter et lire vos conversations personnelles. En toute transparence, Secway Instant Messenger Privacy chiffre vos conversations, identifie de manière certaine vos correspondants et vous avertit en cas de tentative d'usurpation d'identité.

Pour télécharger ces logiciels, rendez vous à l'adresse http://mag.zataz.com

Utilisez la stéganographie

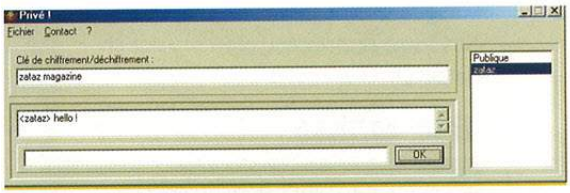
om : Cloak Langage : US Poids : 2,00 mo License : Shareware



Cloak est un logiciel de stéganographie. Il va vous permettre de cacher n'importe quelle information dans une image, de quoi rendre invisibles tous documents que vous ne souhaitez pas voir traîner dans votre ordinateur. Les destinataires de ces fichiers cryptés devront bien entendu posséder eux aussi ce programme pour décoder vos informations cachées.

Chatez en toute sécurité

om : Chat 314 // FR | 0,31 mo | Freeware



Discuter en direct sur le web est devenu un passe temps comme les autres. Seulement voilà, comme vous avez pu le lire dans notre atelier, la sécurité n'y est pas. Le logiciel Chat 314 va vous permettre de chater avec des amis de manière chiffrée.

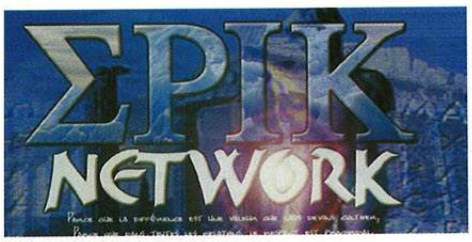
Surveillez votre site web

Nom : Esphp // Fr | 0,01 mo | Freeware

Vous possédez un site web et certaines parties sont secrètes ou réservées. Pour savoir si une personne est venue sur cette page, l'ESPHP est fait pour vous. Ce petit code en PHP vous indiquera l'IP, la provenance, la machine et l'OS utilisé par votre visiteur.

Téléchargez la barre de Zataz Magazine !

Nom : Syllabik Langage : Fr Poids : 8,00 mo License : Freeware



Ce logiciel va vous permettre de chater sur les serveurs IRC. Ecrit par l'équipe d'Epiknet, c'est l'un des meilleurs scripts car ce dernier, de manière simple vous offre toutes les commandes accessibles d'un simple clique. Sécurité oblige, les options pour vous protéger sur IRC sauront vous rassurer.

Sites utiles

Dans chaque numéro de ZATAZ Magazine, nous vous proposons les sites Internet les plus utiles dédiés à la sécurité informatique. Sites français, anglais, de quoi vous faire un petit carnet d'adresses très intéressant. Bon surf !

Kitetoa

Ce site français existe depuis 1998, il est l'une des références dans le domaine de l'actualité dédiée à la sécurité informatique. Le webmaster explique de manière détaillée les bugs et autres failles de sécurité des grandes entreprises qui veulent diriger notre vie. Sans langue de bois, un site INCONTOURNABLE.

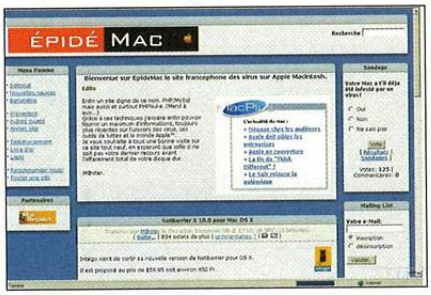
Langue : Français
Url : www.kitetoa.com
Logiciels disponibles : non

Legalis

Ce portail est parfait pour les créateurs de logiciels. Il donne accès à des dizaines d'informations juridiques ainsi qu'à des informations pour protéger vos programmes avec l'Agence de Protection des Programmes, l'APP.

Langue : Français
Url : www.legalis.net
Logiciels disponibles : non

Epidemac



Ce site a pour objectif de permettre aux utilisateurs de Macintosh d'obtenir LE maximum d'informations concernant les virus et indique la marche à suivre pour prévenir ou guérir une attaque virale. Un site complet avec infos et antivirus disponibles en ligne.

Langue : Français
Url : www.epidemac.com
Logiciels disponibles : oui

firewall-net

Ce site est une véritable mine d'or pour les internautes qui souhaitent comprendre ce qu'est un firewall, savoir ou en trouver, gratuits ou non et bien sur comment les configurer convenablement.

Langue : Anglais
Url : www.firewall-net.com
Logiciels disponibles : oui

Attac

Le projet de ce site, réalisé par Marc Blanchard, un Virus-Docteur, est de vous informer sur les attaques virales. Il va vous permettre également de tester vos antivirus avec des codes de tests liés au protocole HTTP. Si vous avez un doute sur l'état de votre machine, un scanner en temps réel peut-être chargé en ligne pour scanner votre PC.

Langue : Français
Url : www.attac.net
Logiciels disponibles : oui

Linux-sottises

Voilà une page qui nous a bien fait rire mais aussi qui nous aura appris des tonnes de trucs et astuces pour Linux. De quoi devenir incollable sur le pingouin. Configuration, mise en connexion sous ADSL, ... Bref du bon et en humour. Que demander de plus !

Langue : Français
Url : www.linux-sottises.net
Logiciels disponibles : oui

L'affaire Kitetoa

Kitetoa, site reconnu pour ses découvertes liées à la sécurité informatique vient d'être condamné à 1 000 euros d'amende avec sursis pour avoir tenté d'aider la marque Tati.
ZATAZ Magazine a suivi le procès. Il ne fait pas toujours bon de dire la vérité sur le web français.

Histoire de bug

En 1999, Kitetoa découvre qu'avec un simple navigateur, Netscape en l'occurrence, il était possible d'accéder à la base de données clients de la société Tati via son site web. Une base de données de quelques 4.000 clients. Prévenu plusieurs fois par e-mail, le webmaster de la société ne semble pas vraiment en avoir tenu compte car un an plus tard les données étaient toujours en ligne. Il faudra attendre novembre 2000, et la parution d'un reportage dans le magazine NewBiz, pour que Tati réagisse. L'article, sur la sécurité informatique, montrait une capture d'écran de la base de données Tati. Base de données illisibles et chiffrées de manière à ne rien montrer aux lecteurs, sauf le fait qu'il était très simple, à cause d'un bug d'un navigateur, de la récupérer.

Histoire d'avocats

Il semble que l'article n'a pas plu à la direction de Tati et le webmaster de Kitetoa reçoit une assignation quelques jours avant les vacances d'été 2001. La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information, la BEFTI, enquête et le parquet émet un avis favorable pour l'ouverture d'un procès en pénal pour "intrusion et maintien frauduleux dans un système de traitement automatisé de données".
Plainte déposée, Kitetoa se retrouve devant les juges, une première fois en janvier 2002. Nous avons assisté à cette audience lors de laquelle il avait été demandé un Euro symbolique et la publication du jugement dans la presse. Pour convaincre le tribunal, Tati avait fait appel à un expert. Ce dernier avait découvert l'utilisation "d'une clé pirate" dixit l'avocate.

Clé inexistante et totalement imaginaire vu que seul le bug du navigateur était responsable. N'importe qui aurait pu le faire et rien n'empêche aujourd'hui de penser que cette base de données a pu être volée par des personnes nettement moins serviables que Kitetoa. "On aurait pu ne pas le poursuivre" expliquera l'avocate de Tati "Mais ce n'est pas parce qu'il y a une porte ouverte que l'on doit y rentrer" rétorquera-t-elle lors de l'audience de février. Le procureur répondra par : "Il peut aussi regarder et dire que l'ameublement à l'intérieur est de très mauvais goût" et que "Cela peut déplaire au propriétaire, mais il n'y a pas de quoi traîner quelqu'un devant un tribunal pénal" avant de conclure : "pour nous (ministère public) l'infraction n'est pas constituée".

Histoire de !

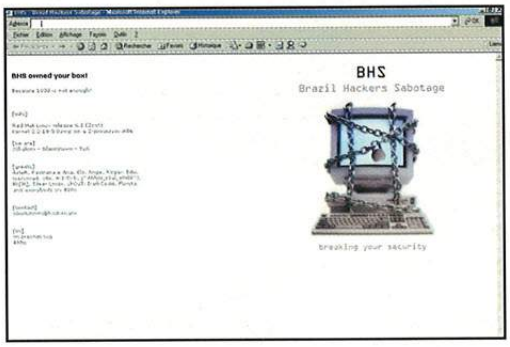
Le jugement a été rendu le 13 février dernier. Tati a été débouté de toutes ses demandes. Le tribunal a expliqué qu'il n'y a eu aucun préjudice pour cette société mais condamne quand même Kitetoa à 1 000 euros avec sursis. Etrange surtout que cela va à l'encontre de ce que demandait le procureur. Bref, encore une histoire qui ne va pas motiver les "internautes" et autres "hackers" à vouloir donner un coup de main lors d'une découverte de faille.

Mais qui t'es toi ?

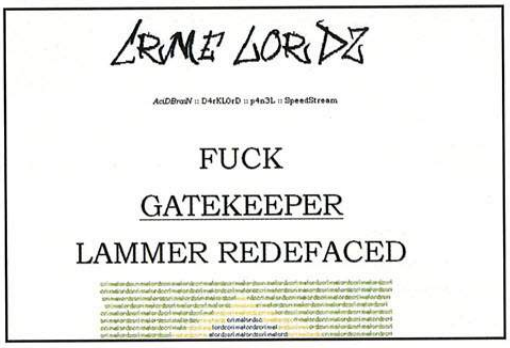
Le site Kitetoa est tenu par un journaliste. Aidé par des internautes, sa mission, démasquer les problèmes informatiques qui touchent les entreprises françaises, ou non, sur le réseau. Le site existe depuis 1997 et a déjà épinglé pas moins de 200 systèmes informatiques. Loin du cliché "hackers" cette fine équipe n'aime pas se faire remarquer, juste mettre le nez là où ça fait mal.
www.kitetoa.com

Les sites piratés du mois !

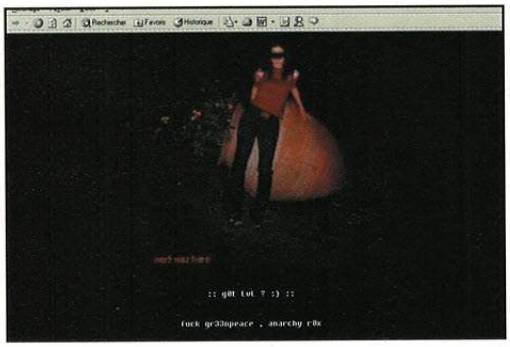
Il s'en passe de drôle sur la toile. Voici notre sélection de sites Internet piratés soit par des script-kiddies en mal de reconnaissance ou bien par des hacktivistes qui utilisent le web comme mur de propagande. Une chose est sûre, l'imagination n'est pas toujours au rendez-vous. Si jamais vous êtes témoin d'un site barbouillé, communiquez nous la capture via l'adresse contact@zataz.com



Cible : medipress.cci.brest.fr
Auteur : Crime Lordz
Notre opinion : Quand des idiots du village s'attaquent à un serveur de la Chambre de Commerce et de l'Industrie de Brest. Le message de ce groupe brésilien est aussi vide que d'habitude.

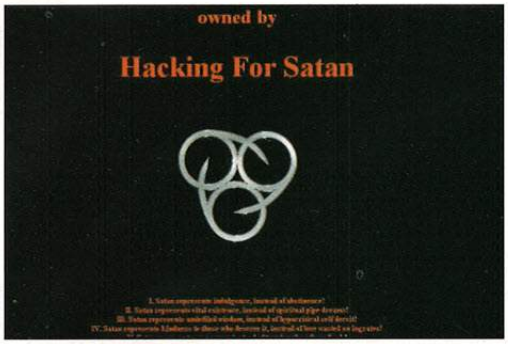


Cible : recherches.mesfinances.fr
Auteur : Brazil Hackers Sabotage
Notre opinion : Encore un groupe brésilien dans un serveur français. Cette fois c'est le serveur "recherche" du site mes finances. Le groupe n'a fait que marquer un territoire qui n'est pas le sien.



Cible : greenpeace.fr
Auteur : Nerf
Notre opinion : L'idiot du village dans toute sa splendeur ! Il attaque le site de Greenpeace France pour y coller la photo de sa copine et noter quelques insultes. Nous ne savions pas que les Thons étaient en voie de disparition.

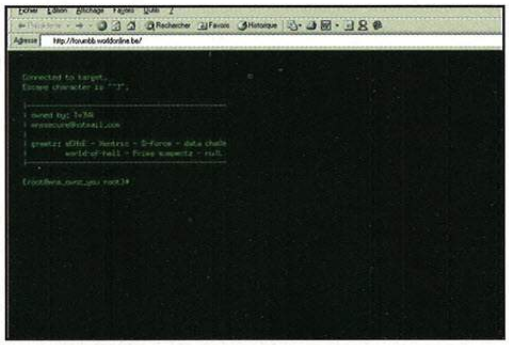
Cible : yamaha.fr
Auteur : Brazil Hackers Sabotage
Notre opinion : Très présent sur le web, ce groupe aime modifier les sites des grandes marques. La dernière victime de taille de ces sales gosses, le site français du constructeur de motos Yamaha.



Cible : chicagoinfo.gov
Auteur : HFS
Notre opinion : Voilà que les adeptes de Satan, vous savez l'ange déchu et cornu, attaquent le site de la mairie de Chicago. Les braves mous du bulbe veulent peut être se présenter aux prochaines élections.

Cible : nysd.uscourts.gov
Auteur : Invisibl3
Notre opinion : Ce pirate brésilien (Ndlr, il y a un nid là bas) s'attaque directement à la cour de justice de New York. Une façon pour lui de prendre ses marques pour son "futur" jugement ?

Cible : jujuy.gov.ar
Auteur : RaFa
Notre opinion : Les troubles qui ont touché le peuple argentin se sont transmis par sites interposés. La page du gouvernement argentin modifié par l'hacktiviste RaFa y est passée. D'après l'auteur de ce piratage, Bush est en grande partie responsable des problèmes qui touchent l'Argentine.



Cible : forumbb.worldonline.be
Auteur : MNS
Notre opinion : Après le serveur business de Worldonline France, dont nous vous relations le piratage dans le premier numéro de ZATAZ Magazine, c'est au tour du serveur forumbb de Worldonline Belgique d'être barbouillé.

Cible : Une trentaine de sites
Auteur : Lion7
Notre opinion : Un petit nouveau qui a signé une trentaine de defacements un peu au hasard. Une signature qui n'a pas du laisser de glace le ministère de l'Intérieur. Ce pirate a signé DST.

Cible : artaban.med.univ-rennes1.fr
Auteur : hax0rs lab
Notre opinion : Hax0rs lab est l'un des groupes de defaceurs les plus actifs du réseau. Avec plus de 400 sites modifiés en 2 ans il laisse un logo anti-nazis sur le site de l'université de Rennes.

COURRIER

Cette page est à toi cher lecteur !. Pose-nous tes questions, propose tes idées, tes remarques et nous y répondrons dans toute la mesure du possible !
Pour nous écrire, une seule adresse : contact@zataz.com

Pompeur sachant pomper !

Je voulais vous féliciter pour le lancement de votre magazine. Je lis vos actualités sur votre site depuis 5 ans et je ne suis vraiment pas déçu du contenu de la version papier. J'ai été étonné, par contre, de voir certaines de vos informations dans des magazines concurrents comme par exemple : «L'affaire du PMU» ou encore «Le site piraté du front national breton» dans un magazine nommé HNM. Qu'en pensez-vous ? Romain (Harnes - 62)

Que te dire à part un grand merci pour ta fidélité. Pour ce qui est du recopiage du magazine que tu cites, on ne peut pas grand chose. Comme nous sommes une des seules source d'information dans le domaine de la cyber-criminalité, nos informations ne sont que trop souvent reprises par ce genre de confrère, visiblement peu enclin à respecter la déonthologie de la presse. Ce n'est de toute façon pas une première. L'éditeur de la revue que tu cites a déjà été assignée par 3 fois au tribunal pour contre-façon ! Ceci en dit long sur ses méthodes. Pour ce qui est de l'affaire du PMU, certains confrères avaient pourtant joué le jeu, comme le quotidien Libération qui a cité Zataz Magazine lorsqu'il a traité le sujet.

E.T... Hacker... Maison...

Salut les enfants ! Pour commencer votre magazine est génial ! Je voulais vous demander plusieurs choses : Peut-on trouver votre magazine dans tous les kiosques ? Ensuite j'ai un pote qui, en scannant le net, est tombé sur un serveur de la NASA, qui peu après a contacté Noos pour se plaindre de l'intrusion. C'est ce qu'a expliqué la personne de Noos qui lui a téléphoné le lendemain. Elle lui a dit que si il n'avait pas décroché, elle lui coupait la connexion et d'autres menaces ont suivi. Je voulais savoir, ce qui allait se passer maintenant. Dj VoDkA via le web

Merci pour le génial, même si c'est un peu exagéré ça fait toujours plaisir. Pour ta première question, ZATAZ Magazine papier se trouve normalement dans tous les kiosques. Si ce n'est pas le cas, demande à ton marchand de journaux qu'il en commande. Pour ta seconde question, ton ami a eu de la chance de ne pas finir sur la liste noire des providers qui lui interdiraient du coup de pouvoir se réabonner, sans parler d'une éventuelle plainte qui aurait pu l'amener devant les tribunaux. Le scan de site web, et surtout celui de sites américains, est considéré comme un début de piratage. En ces temps de paranoïa, suite aux attentats du 11 septembre, il est fortement conseillé d'éviter ce genre de bêtise.

Fautes, fôtes, photeus ...

Bonjour, Je viens de découvrir votre revue que j'ai lue très rapidement, je connaissais déjà votre site. Bravo mais attention aux fautes de frappe ou d'orthographe, aux erreurs :
P 29 : permi avec un S dans le cadre Citroën.
P 30 : La présentation du dernier courrier ne doit pas être la bonne !
P 27 1° ligne : Tous VOUS rendront...
P 28 : tuyauteR dans le cadre 9télécom
Jean-Luc HUET - Paris

Mea culpa. Il est vrai que le premier numéro n'a pas été exempt de fautes et coquilles. Depuis, on a pendu le correcteur et mis en quarantaine notre responsable PAO. Et moi je me suis fouetté pendant quarante jours car je suis le premier responsable.

Vivre dangereusement

Je viens d'acheter le n°1 de Zataz mag. Sincèrement, il donne un réel aperçu du hack sur le Net. Donc, bravo pour ce coup d'essai. En parlant d'autre chose, je me suis amusé (faut vivre dangereusement) à mettre un site de liens en ligne. Dès que je tombe sur quelque chose d'intéressant, je l'y ajoute.
Corsaire - Par e-mail

Attention aux liens hypertextes. toi que derrière un lien ne sommeille pas un site illicite de type Warez, piratage, casino, pédophilie... Tu tomberais sous le coup de la loi avec une fourniture de moyen qui pourrait te mettre devant un juge sans même t'y attendre. Alors vérifie bien chaque adresse de destination de tes liens et n'oublie pas de demander l'autorisation de pointer vers eux.

Non à l'esclavage

Je viens d'acheter votre magazine et je viens de le dévorer entre deux encollages de papier... et surtout pendant que ma copine posait le papier peint ! Continuez vous sortez vraiment du lot ! BdPir par e-mail

Je ne te cache pas que ton courrier nous a bien fait marrer. On imagine cette pauvre fille en train de se battre avec le rouleau et la colle pendant que monsieur lisait notre magazine. Nous espérons que ta femme ne gardera pas une dent contre nous, nous supportons mal les coups de rouleaux.

Taff, job, emploi, stage, etc

Je suis actuellement en 2ème année de DUT informatique et je cherche une entreprise pour mon stage de fin d'étude, je cherche dans le domaine du

Tu es passionné(e) par l'underground, le piratage et le hacking ?
Ecris-nous pour tenter de rejoindre notre équipe !

COURRIER

réseau et de la sécurité informatique. Pourriez vous nous fournir le nom de plusieurs entreprises spécialisées dans ce domaine. Mathieu - Rennes -

Mazette, voilà une vaste question. Comment donnez des noms d'entreprises alors qu'il y en a des centaines en France ? Le mieux pour vous est encore de vous rendre dans votre Chambre de Commerce et de l'Industrie de votre ville pour y demander une liste d'entreprise dans votre secteur d'activité.

Chinoiserie

Bonjour, suite à votre article sur Fluxay, que je souhaitai télécharger j'ai vainement cherché des infos en anglais dans une masse de caractères chinois. Vous est-il possible de fournir l'URL exacte ?

Vous avez été très nombreux à nous demander des informations sur comment télécharger ce logiciel. Le groupe qui a créé ce programme a non seulement bougé l'url quasiment chaque semaine mais a placé un cheval de Troie dans un des exécutables quelques semaines après la diffusion de notre article. Nous nous posions justement des questions à ce sujet. Tu comprendras donc que nous ne pouvons pas te mener à un tel danger.

Aider la justice

Bonjour, me voilà bien pris à mon propre jeu ! Apres avoir voulu faire ma petite loi sur Caramail, je découvre un réseau de plus de 21 boîtes e-mail qui contiennent toutes à ras bord des images pédophiles. Là je suis mal. Que me conseillerais-tu ?

D'abord prévenir les administrateurs de Caramail. Ensuite ne pas hésiter à contacter les forces de l'ordre. Gendarmerie, Commissariat de police ou alors téléphoner au 119 pour expliquer ce que tu as pu trouver. Attention, les citoyens n'ont pas à jouer au justicier. La justice est là pour agir. Donc évite de détruire ou de menacer ces «pédophiles». Moins ils se rendront compte qu'ils sont surveillés et plus il y aura de chance de les arrêter.

A poil sur le web

Bonjour, je suis tombé sur un site web pas comme les autres, ce dernier a modifié les options de mon navigateur Internet Explorer, et a chaque fois que je me connecte, je me retrouve avec des dizaines de sites web qui s'affichent en même temps. Que faire ?
Roland - De Panne - Belgique.

Te voilà victime d'un virus de plus en plus présent sur certains sites pornographiques ou warez. *Trojan.exploit*, son petit nom, n'est pas méchant, sauf qu'il a une fâcheuse tendance a t'obliger à surfer sur des sites qui ne demandent qu'une chose, faire de l'audience. Cela est censé rapporter plus d'argent à leurs propriétaires. Je te conseille d'installer un antivirus qui sera capable de te protéger face à ce genre de problème.

Kim Schmitz

le hoax vivant

Il commence sa carrière médiatique en piratant quelques sites web. Profitant de la méconnaissance des médias sur le sujet, Kim Schmitz, alias Kimble, va s'enrichir sur le dos des crédules. ZATAZ Magazine vous raconte l'histoire de ce hoax vivant.

Le roi de la tchatche

Kim Schmitz a commencé son délire de pirate dés l'âge de 16 ans. Il sera d'ailleurs condamné à deux ans de prison pour piratage informatique. Kimble, son nom de guerre, sera sa signature et l'emblème de trois entreprises qu'il va lancer en 1996. Dataprotect, la plus connue, société de sécurité informatique est aujourd'hui en dépôt de bilan. Kim Schmitz aime l'argent et il est légèrement mégalo. Il suffisait de regarder les petits films en flash le représentant en James Bond du web. Chose rigolote à noter ces films ont été primés lors du Festival International du Film sur Internet (FIFI) en août 1999. Il fera d'ailleurs une demande via son site pour participer au dernier *James Bond*.

Kimble a dépensé sans compter. Tant pis s'il explose sa Mercedes !

Argent, gros nénés et belles cylindrées

Kim aime donc l'argent et aime le montrer. Gros bateaux, gros avions, grosses voitures. Mais avec quel argent au fait ? Ce n'est pas son entreprise qui peut rapporter autant. Non, mais celui des investisseurs qui ont cru au beau baratin de l'imposant allemand. Il faut dire aussi que la presse a aidé Kim Schmitz en lui collant des termes du style "prodige de la nouvelle économie".

On a pu le voir aussi dans la presse française, par exemple dans le magazine Entrevue, fier de dire qu'il avait payé 45 000 dollars d'amende pour conduite dangereuse lors d'une "compétition" automobile de voiture de luxe. Il expliquait aussi dans cette interview, au sujet de la vie des gens qu'il avait pu mettre en danger au volant de son auto : "Ils seraient morts si leur moment était venu".

Coup de pub et coup de bluff

Kim Schmitz commence a intriguer sérieusement le milieu de la sécurité informatique et du business après sa tentative de rachat de la start-up LetsBuyIt.com. Il fera un coup de trop après les attentats du 11 septembre en annonçant la création d'un groupe de hackers anti terroriste nommé Yihat, Young International Hackers against Terrorism. Il annoncera avoir réussi le piratage d'une banque soudanaise hébergeant des comptes d'al-Qaïda. Cette banque, la Islamique Al Shamal Bank - www.shamalbank.com - était victime d'un bug unicode qui avait été découvert 2 mois avant l'annonce de Yihat. Bref, un coup de pub pour sa société mal en point. Quelques gamins tomberont dans le piège. D'autres hackers lui remettront les idées en place, comme Fluffy Bunny, qui donnera son avis directement sur les sites de Kimble " You think you know ? You have no idea - Vous pensez savoir ? Vous n'avez aucune idée ".

Direction la case prison

Ecroué en Allemagne après son expulsion de Thaïlande. Kim Schmitz se cachait dans un hôtel cinq étoiles de Bangkok où il fuyait un mandat d'arrêt délivré le 11 janvier par le procureur de Munich Manfred Wick. Kim Schmitz est notamment soupçonné de délit d'initié après avoir enregistré un bénéfice de plus d'1,1 million d'euros en vendant des actions de la société d'achats groupés par internet en difficultés LetsBuyIt.com. Kim Schmitz doit de l'argent à beaucoup de monde, et pas des plus gentils. Selon le Tageszeitung, trois Russes sont même venus sonner à la porte de Kimble pour venir lui confisquer sa Mercedes 500 au nom d'une dette non remboursée. Belle ambiance sachant que Schmitz annonçait la création de sa propre banque. Il y a une paire d'investisseurs qui ont eu chaud.

On recherche toujours le plus gros.

Pourquoi ne pas acheter le meilleur ?

Format de poche

Petit prix

2,50 Euros

Le 1er magazine Internet de poche
En vente chez votre marchand de journaux

mag.zataz.com