Bimestriel - Belgique : 5,70 Euros - Suisse : 9,50 CHF

N° 10 V 2.0

zataz

zataz

1ère source d'ir ur le piratage

Nouvelle formule avec CD-Rom !

Les sites où trouver des CRACKS special piratage de logiciels !

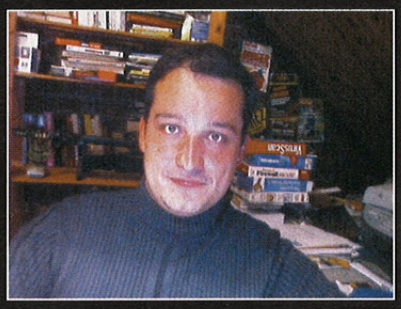
FILMS PIRATES AVEC WINAMP

Terminator 3, SWAT, Matrix 2, découvrez-les en stream vidéo !

Créez un réseau Wi-Fi bétonné contre les pirates !

www.zataz.com

M 05129 - 10 - F: 4,95 € - RD



10 numéros, 100 reportages, articles, interviews, plus de 1000 news totalement exclusives.

Voilà ce que nous vous avons proposé depuis la sortie de ZATAZ Magazine papier en décembre 2001. Un numéro 10 ça se fête, d'où en plus de votre magazine préféré, un CDrom concocté spécialement pour vous, contenant des centaines de logiciels de sécurité, des softwares pour faire vos copies de sauvegarde...

ZATAZ Magazine papier 10, c'est aussi plus de reportages décalés. On ne vous apprendra pas à devenir un hacker, un super méga flibustier du web, on laisse cela à ceux qui fantasment sur ce genre de chose. On préfère gratter là ou personne ne vous a déjà entraîné. Comme par exemple du côté de la Patrouille de France, les pros de l'aviation qui ont été perturbés par des pirates. Nous sommes aussi allés jeter un oeil dans les écoles françaises du 21ème siècle. Des écoles qui espionnent aussi leurs élèves... pour leur bien. Espionnage encore, avec le traçage de nos téléphones portables et une découverte sur internet qui nous fait regarder notre GSM d'un autre oeil. Piratage de films aussi, avec une source de diffusion pas comme les autres via le logiciel Winamp. Découverte aussi des cracks, ces petits logiciels qui font la peau aux protections de nos logiciels. Nouvelle rubrique également, adieu la page hacked, bienvenue à la page HaideD.
Voilà, en quelques lignes, ce que vous propose ce 10ème opus. On vous laisse savourer le reste.

Bonne lecture, on se retrouve l'année prochaine, en janvier 2004.

Damien Bancal

SOMMAIRE

Zataz Magazine : 61, rue Jouffroy d'Abbans, 75 017 Paris. Fax : 01.40.53.86.44 E-mail : mag@zataz.com, web : www.zataz.com
Chef de la rédaction : Damien Bancal
Ont collaboré à ce numéro : Alix Bernaud, Christophe Fantoni, Eric Romang, Christophe Schleypen, John Jean, Mathieu Spolix, LiNuX.
Correspondants : Nita et Ngyuen - correspondants Hong-Kong. Nihiatu - **Correspondant à Dheli.** Guillaume, Sam et Lucile - **Correspondants aux USA.** Jeff et David - **Correspondants à Tel-Aviv.** Mike - Banglasdesh.
Conception graphique : Patrice Guyonnet **CORRECTRICE :** MARIE DEVIGNAC **Impression :** Léonce Deprez, Béthune
Distribution France : NMPP - Belgique : AMP **Commission paritaire :** 0707 T 81854 Dépôt légal à parution
Service des ventes : Distrimédias, Mr. Patrick Didier. tél. : 05.61.72.76.72 - fax : 05.61.43.49.50
Directeur de la Publication : Charles Daleau
Editeur : Mediastone, 61 rue Jouffroy d'Abbans 75 017 Paris . Siret :422990015200019 - Code APE : 221E

CDROM ZATAZ MAGAZINE 10

Bientôt Noël, et avec ce 10ème numéro de ZATAZ Magazine, nous avons devancé le barbu et ses rennes avec un CDrom bourré à cracker d'outils de sécurité, de logiciels, de démos, de jeux inédits... Pour en profiter, placez votre CDrom dans votre lecteur et suivez le guide. La galette en plastique va lancer automatiquement le menu.

KASPERSKY ANTI HACKER 1.5.92.0

Eure'net et Kaspersky vous offrent la possibilité de tester Kaspersky Anti Hacker version 1.5.92. Ce logiciel est un pare-feu personnel, destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus, provenant d'un réseau local adjacent ou de l'Internet. Après avoir installé le soft sur votre machine, installez la clé d'activation nommée : 00058CF9.

GAMERZ

Une dizaine de jeux totalement inédits pour votre machine. D'abord, de grands classiques revisités par des demomakers. Un jeu de tir comme Turrican ou un jeu de plate-forme nommé *Rick Dangerous* va rappeler de sacrés souvenirs aux plus vieux d'entre vous. A n'en pas douter, les plus jeunes vont adorer. Pour les amateurs de jeux de rôle, découvrez aussi *Retour à Actarius*, d'Alain TEXIER. Un long jeu de rôle accessible à tous ! Retrouvez les 4 miroirs magiques *d'Actarius* afin de les orienter et ainsi détruire la menace pesant sur cette planète.

SIMP FAMILY

La société française Secway vous propose de tester ses logiciels de chiffrement pour les pagers de MSN, AOL, Yahoo, ICQ. Simp vous permet d'utiliser les messageries instantanées en chiffrant vos conversations. Il sécurise aussi bien les messages que le transfert de fichiers, pour MSN Messenger uniquement, et s'administre facilement par GPO.

ANTIVIRUS

Près de 200 antivirus pour contrer Sobig, Yaha, Nimda, Potok, Lovegate, Blaster Family. Ces antivirus sont tous dédiés à un microbe numérique précis, ce qui vous permettra en cas de problème, de pouvoir calmer l'ardeur du worm en question. Les antivirus sont au crédit de Panda Software, Bitdefenders, Symantec, Sophos, ZATAZ Mag...

DEMO'NIAK

Vous avez été plus de 15 000 à nous demander des démos et encore des démos. D'ailleurs, notre serveur FTP s'en souvient encore grâce aux pointes atteignant plusieurs centaines d'utilisateurs par minute pour télécharger certaines productions présentées. Voilà donc qui devrait vous plaire avec pas moins de 100 Mo de démos, intros, cracktros, Music Disk, E-zines...

TRAINERS

Gagner, avoir des vies, de l'énergie infinie dans vos jeux favoris, voilà ce que propose la partie Trainers. Nous vous en proposons une centaine, pour des jeux récents ou plus anciens. De quoi devenir les boss des levels.

ANTI-VIRUS / ANTI-HACKER

www.antivirus-france.com

E-mail : info@antivirus-france.com

Kaspersky Anti-Virus

Personal / Pro (Windows)

Workstation / Serveur (Windows / Linux)

Eur'Net

Nous répondons à toutes vos demandes d'information et de tarifs.
Et nous vous proposons des versions d'évaluation
4, route de la Fossery - F-27220 LA BOISSIERE
Tél : +33 (0) 232 366 364 - Fax : +33 (0) 232 366 367

Secret défense

Si vous êtes un amateur de la console de jeu de Microsoft, la Xbox, et que vous êtes relié au Xbox live, vous n'avez peut-être rien senti. Si vous êtes un possesseur d'une Xbox modifiée, contenant éventuellement Linux et que vous êtes connecté au live, vous avez dû certainement vous demander pourquoi plus rien ne fonctionnait depuis la mi-septembre. La réponse est simple. Microsoft met à jour la console connectée au Xbox live, sans prévenir personne. Les buts avoués : corriger un bug et éliminer les consoles qui utilisent des puces et des systèmes Linux qui ne sont pas autorisés.

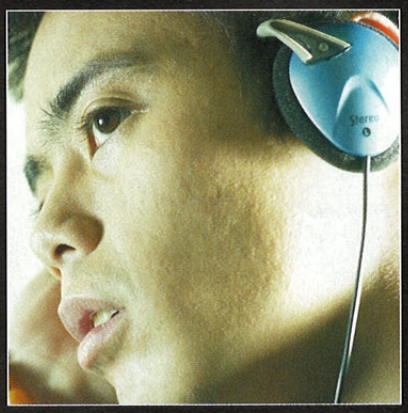
Vend PC et données sensibles

Une banque se sépare de ses ordinateurs et de ses informations sensibles sur un site de vente aux enchères. L'histoire vient d'être révélée par un étudiant de New York de 26 ans, qui venait d'acheter des ordinateurs via le site de vente aux enchères eBay. Les machines étaient vendues par la banque Ecosys Canada Inc. Seulement, cette dernière n'avait pas fait le ménage. Geoff Ellis, l'étudiant en question, a trouvé sur les disques durs les noms, les adresses et les numéros de téléphone de plusieurs centaines de clients de la banque. Cerise sur le g.teau - sinon cela n'aurait pas été drôle, il avait aussi les informations liées à leurs comptes bancaires.

Donner, c'est donner, reprendre...

Le site britannique de jeux online tombola.com, a fait gagner tous les internautes le week-end du 15 septembre dernier. Un pépin informatique que personne n'a encore vraiment compris. Les participants au jeu i:scratch ont tous gagné 5 000 livres sterling, soit plus de 7 000 euros. Seulement la société britannique en charge du site a envoyé un mel quelques heures plus tard, pour s'excuser d'une erreur dans le logiciel de traitement. Comme d'habitude, il suffit de lire les conditions générales pour se rendre compte que l'internaute n'a rien à dire : "le site n'est pas responsable des échecs techniques". La direction a fait un tirage au sort parmi les joueurs. 100 d'entre eux ont reçu... 70 euros. C'est le second problème "informatique" pour ce site de jeux online, mais vu qu'ils ne sont pas responsables !

LE SILENCE EST D'OR



Arista Records, filiale de BMG, a testé une nouvelle protection musicale qui a pour but de protéger ses albums musicaux. Le test, grandeur nature, a débuté aux U.S.A. le 23 septembre dernier via l'album d'Anthony Hamilton.
La protection permet d'écouter l'album sur n'importe quel support : chaÔne hi-fi, consoles, baladeurs... mais ne permet pas de copier le contenu du CD sans être obligé de griller plusieurs cdr. La technologie vient de chez SunnComm Inc, entreprise basée à Phoenix.
Point intéressant : c'est la première fois qu'un album est équipé d'une telle protection sur le marché américain. Les pirates ont mis 7 jours pour se payer la tête de cette protection.

DÉCOLLAGE. .. IMMÉDIAT !

Etrange série ! Après Air Canada et les aéroports de Chicago ainsi que celui de Dallas, c'est au tour de la compagnie aérienne British Airways d'être collée au sol en raison d'un problème informatique. Des centaines de clients ont vu leurs vols annulés ou retardés après un échec informatique. L'ensemble des ordinateurs de la compagnie, à travers le globe, est parti en carafe. Le problème est survenu dans le centre informatique de British Airways basé près de Heathrow.

MATERNELLE SOUS SURVEILLANCE

Un australien a été pris la main dans le sac par des parents à la porte d'une maternelle. Equipé d'un téléphone-appareil-photo, l'homme photographiait les enfants en train de jouer. Agé de 20 ans, le photographe se retrouve devant les magistrats d'Ipswich. Il est accusé de « traitement indécent » sur enfants de moins de 16 ans.

SANS BLAGUE ?

Une étude publiée par AT&T Labs vient de démontrer que plusieurs des films piratés qui circulent sur internet ont été mis en circulation par des "pirates" travaillant pour Hollywood. Sacré scoop que voilà ! Nous vous en parlions il y a 9 mois dans ZATAZ Magazine papier numéro 2. D'après cette étude, près de 80 % des 300 films proviennent de sources internes des majors. Mega scoop aussi ! Certaines des copies comportent des timers, des chronomètres, prouvant que le film a été copié sur un banc de montage, voire en salle de projection de test. Ca aussi on vous l'expliquait dans ZATAZ Magazine 2. Les "experts" de cette étude ont pris le cas du film Hulk qui aurait été piraté à partir de l'agence de communication chargée de la promotion du film en question.

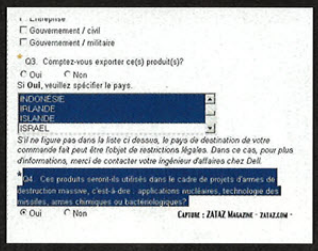
PERVERS PÉPÈRE

Nous vous parlions cet été du cas d'un pirate informatique pas comme les autres. Le gars, pseudo Deepsy, s'était spécialisé dans l'escroquerie visant des sites pornos. Ce pirate de 20 ans, Pavel Vladislav, a été arrêté en IsraÎl. Il exigeait des webmasters de sites pour adultes 1 500 dollars, autant d'euros. En contrepartie, il ne piratait pas le site et ne revendait pas les bases de données qu'il avait pu voler. Trois sociétés ont déposé plainte. L'une d'elles, SilverCash, qui n'avait pas souhaité payer, s'était vue attaquer par un déni de service, 750 millions de hits par jour, qui ont planté son serveur durant plusieurs jours

SANS DOMAINE FIXE

La B.P.I, comprenez l'association des majors du disque du Royaume-Uni, qui peut être comparée à la RIAA de l'Oncle Sam, va tenter de pirater les noms de domaine des sites proposant des mp3 pirates. Lors d'une réunion récente, il a été révélé que la British Phonographic Industry est entrée en contact avec Nominet, société responsable de l'enregistrement des noms de domaine au Royaume-Uni.La B.P.I. souhaite rendre obligatoire le contrôle des enregistrements des noms de domaine. Dans le pire des cas, elle se donnera le droit de prendre le contrôle du nom de domaine d'un site pirate. Les noms de domaine enregistrés avec un faux mel seront systématiquement récupérés par la B.P.I. A suivre donc...

SALUT, MOI C'EST LADEN, BEN LADEN



Certains sites prennent au pied de la lettre les lois en vigueur pour contrer les vilains pirates et autres terroristes. En allant sur le site DELL, constructeur informatique de renom, il a été découvert un questionnaire des plus... bizarres. Alors si vous êtes irakiens, que vous ayez l'intention de vous servir du matériel acheté via la boutique online de DELL pour des projets d'armes de destruction massive, c'est-à-dire : applications nucléaires, technologie des missiles, armes chimiques ou bactériologiques, passez votre chemin. (Merci à tony29montana).

WU SHU

Taîwan s'inquiète de l'agressivité croissante des pirates chinois. Le gouvernement taîwanais accuse la chine d'accroÓtre sa guerre de l'information à l'encontre de l'Óle. Utilisation de pirates, de virus et de trojan pour agir. Les victimes pour le moment : 30 organismes gouvernementaux (police, ministère de la défense, la banque centrale...) et 50 entreprises privées.

BIP ! BIP !

Les amateurs d'overcloking vont adorer. Des informaticiens russes ont réussi la transformation d'un Duron AMD en un Athlon. Il semble que le L2 cache de 256 KB n'est pas verrouillé.
http://www.xbitlabs.com/news/cpu/display/20030908004407.html

ALLO ? SUITE...

Un exploit à pirate serait-il dans la nature ? Une nouvelle compagnie téléphonique se retrouve sourde et muette après un problème informatique. Les services de téléphonie mobile de la filiale de Deutsche Telekom T-Mobile, basée à Francfort, a vu son service coupé plusieurs heures le 9 septembre. Motif de la panne : coupure de courant. C'est dingue le nombre de problèmes électriques en ce moment ! C'est bientôt la fin du monde ou quoi ?

AUDIT SOIT QUI MAL Y PENSE

Alex-ploit, de la Alex family white hat francophone, nous a fait une petite démonstration sur la manière dont un site web peut se faire pirater uniquement en passant par le PC d'un internaute, sans même qu'on s'attaque à la sécurité du site à pirater. L'exemple a été fait avec ZATAZ Magazine. Un petit audit qui, si on n'y prend pas garde, peut permettre à un défaceur, voire un espion, de passer par votre site.
1ère étape : chercher à savoir qui possède les mots de passe du serveur ciblé : webmaster, journalistes...
2ème étape : après avoir récupéré l'IP des protagonistes, chercher qui est sensible à l'une des nombreuses failles de Windows : Netbios, Rpc... L'un de nos collaborateurs avait des fuites :)
3ème étape : rechercher le logiciel de ftp qu'utilise l'internaute ciblé, et décrypter login et mot de passe.
4ème étape : si le décryptage est réussi, le pirate peut modifier ou voler les informations du site gr,ce aux précieux sésames ainsi récoltés.
Le test qu'a effectué Alex-ploit avec ZATAZ Magazine aura pris à peine 20 minutes, modification et création de la page index comprise dans le répertoire faillible. Bien sûr, nous avions mis en place plusieurs failles pour que ce test fonctionne, et utilisé un logiciel de ftp faillible. Un test réussi qui montre une fois de plus qu'il est plus que conseillé de bien vérifier vos machines, de les patcher et de ne pas hésiter à informer et former vos collaborateurs. Une erreur humaine est si vite arrivée.

Minority report

Les policiers de la ville de Pratt, Kansas du sud, utilisent un système de caméras sans fil qui permettent de contrôler, à distance, des points chauds de la ville. Banques, parcs, ruelles... Il y en aura pour tout le monde. Le système permet aux officiers en patrouille de "regarder" à l'intérieur d'une banque, par exemple, si une alarme se déclenche. Le système global va coûter 225 000 dollars, autant d'euros. Les transmissions fonctionnent sur une bande radio de 2.4 giga-octets qui couvre approximativement 5 kilomètres carrés. Les caméras fournissent les images via un accès haut débit internet dans les voitures de police.

Sale gosse

Un gosse de 14 ans a reconnu avoir diffusé sur internet plusieurs centaines de dossiers de clients d'une entreprise de Nouvelle Zélande. 985 dossiers du fournisseur d'accès Net4U. Le gamin semble avoir été employé par cette société. Il aurait agi ainsi "par rancune". Les informations ainsi diffusées sur deux sites web incluaient les noms, des adresses, des numéros de téléphone, des adresses mails ainsi que des mots de passe et les numéros de cartes de crédit des clients, avec les dates d'expiration.

Chéri, j'ai le DVD qui fume !

Nous vous expliquions voilà presque un an le projet de Disney de commercialiser des DVD auto destructibles, afin de contrer le piratage de films. Le projet vient de devenir réalité avec la vente des premiers titres Walt Disney via sa branche vidéo Buena Vista. Quelques titres seulement pour le moment, qui utilisent la protection appelée EZ-D. Une fois le DVD sorti de sa boÛte, un composant chimique altère le DVD en 48 heures. Pour 7 dollars, les clients peuvent donc acquérir un film qui ne sera plus exploitable deux jours plus tard. La o˝ cela risque de devenir saignant, c'est dans le cas o˝ des groupes d'hacktivistes s'amuseraient à casser les boÛtiers, sous vide, directement dans les magasins pour accélérer líaltération antipirate.

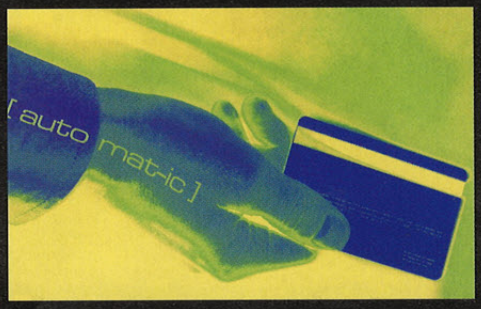
Allo ?

Piratage ? Bug ? 60 000 clients du fournisseur de téléphonie mobile Qwest sont restés sourds et muets durant 5 heures le 3 septembre dernier. Le FBI enquête pour tenter de comprendre comment ce "problème" a pu couper toute communication dans le Comté de Snohomish, Etat de Washington. Il semble que la société Verizon ait elle aussi été touchée dans le Comté de Whatcom.

QUI LU KREW !

Deux britanniques du groupe de pirates Thr34t-Krew, arrêtés en février dernier vont passer devant les juges. Ils sont accusés d'avoir créé et utilisé un cheval de Troie nommé TK. Ils ont été appréhendés dans le nord de l'Angleterre par les cyber flics de sa gracieuse majesté, la NHTCU, National High Tech Crime Unit. Jordan Bradley, 20 ans, et Andrew Harvey, 22 ans, auraient occasionné avec leur cheval de Troie pas moins de 5.5 millions de livres sterling, soit 7.8 millions d'euros de dég,ts. Le trojan utilise la célèbre faille Unicode IIS qui a visé en 2001 les serveurs sous Windows NT. Cette faille avait été utilisée par le virus Code red.
http://www.zataz.com/zatazv7/news.php?id=2348

CASE PRISON



Un technicien informatique de Checkline plc vient d'écoper de 9 ans de prison pour avoir volé 9 000 cartes bancaires. Il avait revendu son larcin à un groupe de pirates qui s'en est servi au point de détourner 2 millions de livres sterling, soit 2.8 millions d'euros. Sunil Mahtani, 26 ans, a plaidé coupable pour avoir téléchargé presque 10 000 numéros de cartes de crédit du système Checkline. Cerise sur le g,teau (façon de parler) le juge lui a ajouté 2 ans de prison ferme car il a été découvert que cet escroc avait téléchargé des images pédophiles. Deux des complices de Sunil ont écopé de 4 ans de prison. Huit autres personnes doivent encore passer à la moulinette de la justice.

C'EST PAS MOI, C'EST LUI

Alors que des experts annoncent la probable arrivée d'une nouvelle version du virus Sobig, d'autres expliquent que les blocages internet liés à ce virus sont dus aussi aux alertes des antivirus. Le fondateur de f-prot, Fridrik Skulason, a expliqué que les alertes par mels des logiciels antivirus, alertes liées au virus Sobig, ont ralenti plus encore les connexions que le virus lui-même. M. Skulason conseille aux administrateurs de configurer leur logiciel antivirus pour ne pas faire sortir ce genre d'alerte.

1+1+1+1

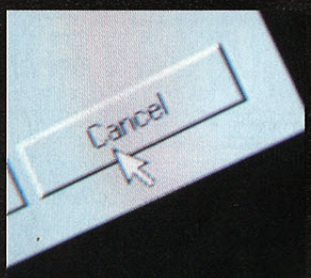
Il se nomme 60X1 et propose un site web à l'url comportant pas moins de 60 chiffres 1. Le contenu de son site est une sorte d'hommage au chef du gouvernement italien Silvio Berlusconi et au premier ministre britannique Tony Blair. Enfin, hommageÖ façon de parler. L'auteur du site a reconstitué le livre "la guerre des mondes" de HG Wells avec comme slogan : "Freedom Is Not Free When Freedom Fries Are Not Free !". A noter que la page change selon líactualité. (source Coromputer)
http://www.1111111111111111111111111111111111111111111111111111111111111111.com

GROS POISSONS Y BECQUE SU L'TARD.

Le premier pirate de la Martinique condamné à de la prison. Olivier Marshall, 36 ans, a été arrêté fin août par les policiers de l'office central de lutte contre la criminalité technologique de l'information et de la communication, l'OCLCTIC, pour avoir piraté l'hébergeur DSI. Il avait signé cls_fwi sur une douzaine de sites comme site-creation.net, abcimmo.mq, traiteurs.com, avocat-martinique.com, location-martinique.com, rhums.com, pompes-funebres.com. Il avait laissé comme message : "ADMIN : c'est un bon jour pour toi... Hahahahaha :-) This hacking does not aim at destroying information or inflicting any material damage on the owner of this server... The aim is to demonstrate low professional qualities (lameness) of the system administrator. I didn't delete anything. Backup of index.html is hacked.html. MARTINIQUE RLZ. (c)opirate French Warez Indies Since 1997". Il a été condamné à 2 mois de prison avec sursis et 3000 euros d'amende.

IDIOT SANS NOM

La police américaine a mis la main sur John Zuccarini, un internaute qui a enregistré près de 3 000 noms de domaine ayant pour but de détourner des adresses internet de grandes marques. Les urls ainsi modifiées renvoyaient sur des sites pornographiques. Le problème pour cet escroc, c'est qu'il a aussi détourné des noms de sites pour enfants, comme le site web du parc Disneyland qu'il a transformé en "dinseyland". Zuccarini tombe sous le coup de la loi sur les marques qui interdit aux internautes de créer des noms de domaine induisant en erreur. La police estime que son système lui rapportait 1 million de dollars par an. Il risque quatre ans de prison et 250 000 dollars d'amende.



CHAT ÉCHAUDÉ...

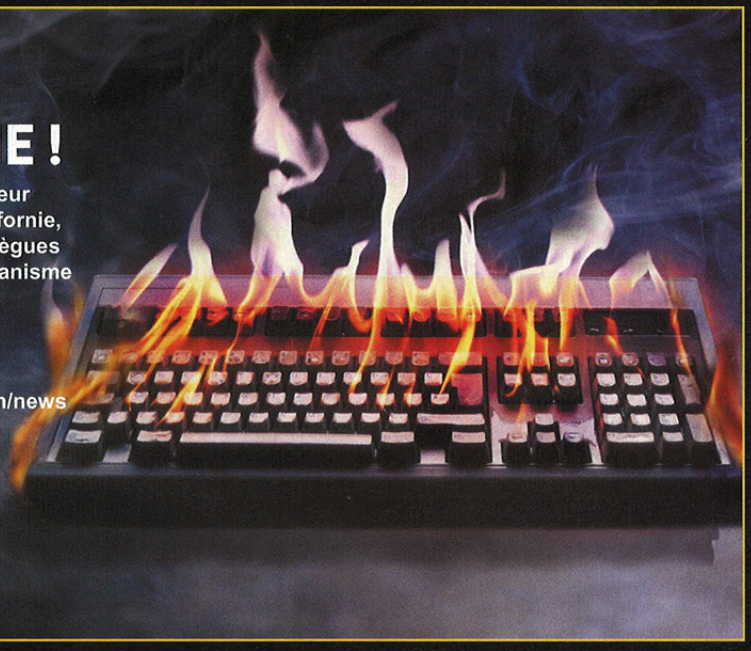
Nous vous expliquions cet été que les auteurs allemands du logiciel CloneCD devaient arrêter la production de leurs logiciels de gravure de CD et de DVD. La loi sur la protection des droits d'auteurs ayant changé en Allemagne, CloneCD et CloneDVD sont devenus outre-Rhin illégaux. Il semble que CloneCD et DVD vont continuer à vivre... à Antigua. La société SlySoft, basée dans cette ville du Guatemala, va reprendre le bébé à son compte. Elle propose déjà le logiciel AnyDVD.

MÊME PAS PEUR !

Microsoft doit encore corriger 30 importantes failles ouvertes aux pirates. Selon le chercheur Thor Larholm de Solutions PivX, Microsoft doit encore rapiécer 30 défauts de sécurité uniquement pour Internet Explorer. Dans la liste : utilisation du bouton "annuler" d'une fenêtre d'alerte pour bloquer le navigateur, une autre faille permet de voler des cookies et des données sensibles, ou encore une légion de moyens d'exécuter des codes arbitraires.

CHÉRI, TON PC FUME !

Michel Sailor est professeur à l'Université de la Californie, basée à San Diego. Ses collègues et lui ont développé un mécanisme qui permet de détruire un ordinateur, un téléphone portable, en envoyant un message à distance. http://www.newscientist.com/news/news.jsp?id=ns99991795



ALLO, ZATAZ ?

Vous avez été nombreux à nous demander une hotline pour vos questions, suggestions, informations, etc... Voilà qui est fait. Vous pouvez joindre l'équipe de ZATAZ Magazine par téléphone au 0892 680 631 suivi du numéro de poste : 8821# de 10h à 19H toute la semaine. Coût de l'appel : 0.34 euro. A noter que tous les 50 appels, un abonnement à ZATAZ Magazine est offert.

SUIVEZ LE GUIDE

L'union des fabricants vient d'éditer un guide destiné à faciliter la conduite des enquêtes et la rédaction des procédures des officiers de police judiciaire, les OPJ. Ce manuel est destiné aux policiers chargés de la répression en matière d'atteinte aux droits de propriété industrielle, littéraire et artistique. A noter que ZATAZ.COM vous propose une visite virtuelle, en images, du musée de la contrefaçon.

CALLTO://

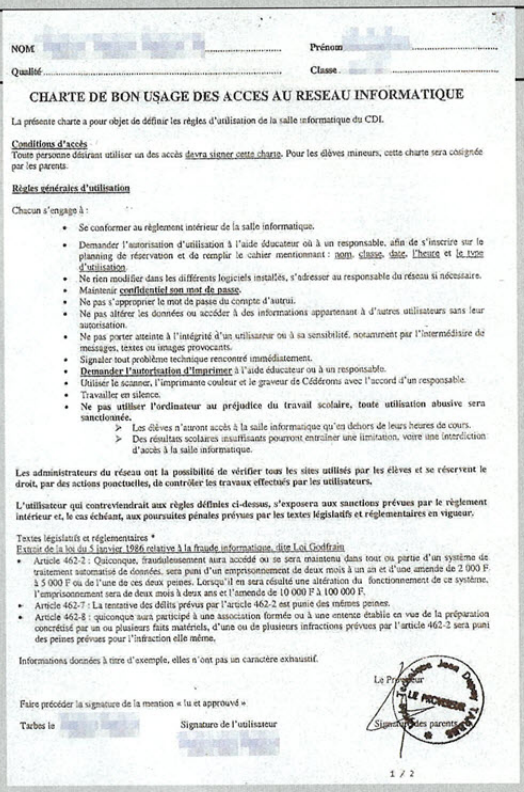
La téléphonie via le Peer to Peer, possible gr,ce au père de KaZaA. Le système se nomme Skype, www.skype.com, un service de discussion par la voix, qui devrait être révolutionnaire car il est basé sur le principe du P2P. Il annonce un service supérieur à Dialpad ou encore Net2Phone. Chiffrement à 256 bits AES, tourne sous Windows 2000 ou XP. 128 Mo de mémoire et un PC tournant au minimum à 400 MHz sont conseillés.

DYNAMIQUE

Vous avez une connexion internet ADSL ou par c,ble, vous désirez faire de l'hébergement de votre site web, irc, ftp, serveur de jeu, sur votre ligne ADSL ou c,ble, malheureusement votre adresse IP change à chaque connexion. En solution, ZATAZ vous propose de vous créer gratuitement un domaine du type : mon-nom.zataz.xxx - nickname.zataz.xxx - cequevousvoulez.zataz.xxx.
Ce service, gratuit, vous permettra de joindre votre serveur même si votre adresse IP change, puisque la mise à jour de votre adresse IP sur votre domaine est effectuée en temps réel. Vous pourrez ainsi créer jusqu'à 5 DynZATAZ via votre compte. Pour en profiter, direction ZATAZ.COM.

VOTRE ÉCOLE VOUS ESPIONNE !

ALORS QUE L'INFORMATIQUE ENTRE EN FORCE DANS LES ÉCOLES, QUE LA RUPTURE NUMÉRIQUE SE FAIT DE PLUS EN PLUS DISCRÈTE, LES ÉCOLES DOIVENT FAIRE FACE AUJOURD'HUI À DE NOUVEAUX PROBLÈMES. PIRATES, ESCROQUERIE, CONTREFAÇON. NOUS AVONS DÉCOUVERT COMMENT CERTAINES ÉCOLES, DONT CERTAINES SONT FRANÇAISES, ESPIONNENT LEURS ÉLÈVES... POUR LEUR BIEN.



NOM ..... Prénom .....

Qualité ..... Classe .....

CHARTE DE BON USAGE DES ACCES AU RESEAU INFORMATIQUE

La présente charte a pour objet de définir les règles d'utilisation de la salle informatique du CDI.

Conditions d'accès
Toute personne désirant utiliser un des accès devra signer cette charte. Pour les élèves mineurs, cette charte sera cosignée par les parents.

Règles générales d'utilisation

Chacun s'engage à :

- Se conformer au règlement intérieur de la salle informatique.
- Demander l'autorisation d'utilisation à l'aide éducateur où à un responsable, afin de s'inscrire sur le planning de réservation et de remplir le cahier mentionnant : nom, classe, date, l'heure et le type d'utilisation.
- Ne rien modifier dans les différents logiciels installés, s'adresser au responsable du réseau si nécessaire.
- Maintenir confidentiel son mot de passe.
- Ne pas s'approprier le mot de passe du compte d'autrui.
- Ne pas altérer les données ou accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation.
- Ne pas porter atteinte à l'intégrité d'un utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants.
- Signaler tout problème technique rencontré immédiatement.
- Demander l'autorisation d'imprimer à l'aide éducateur ou à un responsable.
- Utiliser le scanner, l'imprimante couleur et le graveur de Cédéroms avec l'accord d'un responsable.
- Travailler en silence.
- Ne pas utiliser l'ordinateur au préjudice du travail scolaire, toute utilisation abusive sera sanctionnée.
  - Les élèves n'auront accès à la salle informatique qu'en dehors de leurs heures de cours.
  - Des résultats scolaires insuffisants pourront entraîner une limitation, voire une interdiction d'accès à la salle informatique.

Les administrateurs du réseau ont la possibilité de vérifier tous les sites utilisés par les élèves et se réservent le droit, par des actions ponctuelles, de contrôler les travaux effectués par les utilisateurs.

L'utilisateur qui contreviendrait aux règles définies ci-dessus, s'exposera aux sanctions prévues par le règlement intérieur et, le cas échéant, aux poursuites pénales prévues par les textes législatifs et réglementaires en vigueur.

Textes législatifs et réglementaires *
Extrait de la loi du 5 janvier 1986 relative à la fraude informatique, dite Loi Godfrain

- Article 462-2 : Quiconque, frauduleusement aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données, sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 F. à 5 000 F ou de l'une de ces deux peines. Lorsqu'il en sera résulté une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10 000 F à 100 000 F.
- Article 462-7 : La tentative des délits prévus par l'article 462-2 est punie des mêmes peines.
- Article 462-8 : quiconque aura participé à une association formée ou à une entente établie en vue de la préparation concrétisé par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par l'article 462-2 sera puni des peines prévues pour l'infraction elle même.

Informations données à titre d'exemple, elles n'ont pas un caractère exhaustif.

Faire précéder la signature de la mention « lu et approuvé »

Tarbes le Signature de l'utilisateur

Le Proviseur Jean Dupuy LE PROVISEUR

Signature des parents

1 / 2

Le règlement de la salle informatique d'une école française.

SALLE INFORMATIQUE SOUS SURVEILLANCE

Plusieurs de nos lecteurs nous ont mis la puce à l'oreille. Les règlements intérieurs de leurs écoles venaient d'être agrémentés de nouveaux alinéas spécialement concoctés pour les salles informatiques. Prenons l'exemple d'un lycée professionnel de Marseille. Le règlement stipule que *"les administrateurs réseaux ont la possibilité de vérifier tous les sites utilisés par les élèves et se réservent le droit par des actions ponctuelles de contrôler les travaux effectués"*. Contrôler les travaux ? Nous avons posé la question à la direction de cette école qui n'a pas souhaité nous répondre. Ce n'est pas la seule. Nous avons eu la preuve que des sniffeurs étaient utilisés dans certaines écoles du nord de la France. Nous avions deux cas concrets mais après notre passage, les machines ont été nettoyées. L'un des surveillants que nous avons rencontrés lors de notre enquête nous a précisé que les règlements étaient de plus en plus stricts. Le lycée Jean-Dupuy à Tarbes va jusqu'à rappeler aux élèves la loi Godfrain : *"Tout maintien ou accès frauduleux peut provoquer 1 an de prison"*.

BIENVENUE À GATTACA

La direction du collège Joliot Curie, dans le Var, a mis en place plusieurs systèmes informatiques pour contrôler les élèves et éviter les fraudes. D'abord les bulletins de note peuvent être contrôlés via internet par les parents. Les absences sont aussi notifiées en temps réel. Pour couronner le tout, le contrôle d'accès à la cantine est effectué par un système biométrique. Les gamins doivent entrer un mot de passe et placer leur main sur le détecteur pour se sustenter. Le système contrôle 90 points de la main. Le directeur explique que cela permet d'importantes économies. 30 % des cartes d'accès étaient habituellement perdues les années précédentes.

L'INTERCEPTION DE DONNÉES SUR LE RÉSEAU D'UNE ÉCOLE

La pratique du "sniff", qui consiste à intercepter les données circulant sur un réseau par un responsable de celui-ci via un keylogger, un sniffeur, se heurte à différentes législations destinées à protéger les données concernées. Ces législations concernent à la fois la protection de la vie privée et la protection des données à caractère personnel.

L'article 226-15 dans son alinéa deux, prévoit explicitement le cas des télécommunications : *" Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions"*.
Ces dispositions instaurent un régime strict de secret relatif à ces correspondances émises par la voie des télécommunications. La peine prévue par l'article 226-15 alinéa premier, concernant toute atteinte au secret des correspondances est *" d'un an d'emprisonnement et de 45.000 euros d'amende. "* On peut donc voir que les peines sont très lourdes. En application de ces dispositions le principe est donc simple : il est interdit d'intercepter les correspondances.

LA VIE PRIVÉE

La notion de vie privée prévue par l'article 9 du code civil est une notion à géométrie variable. En effet, comme elle n'est pas définie strictement par les textes, il appartient au juge de définir au cas par cas son contenu. La jurisprudence estime qu'est illicite toute immixtion arbitraire dans la vie privée d'autrui et que le fait de se faire épier, surveiller et suivre, est une immixtion illicite.
Concernant l'interception de données sur le réseau de l'école, on peut légitimement penser que des communications telles que sur des chats par exemple, sont clairement protégées par la vie privée, ensuite pour le reste l'interception du surf des internautes peut être, en fonction des circonstances, rattachée ou non à la vie privée. Le régime juridique permet, comme pour le secret des correspondances, de s'opposer à l'interception et à l'utilisation des éléments de la vie privée. L'article 9 du code civil autorise ainsi le juge à prendre toutes les mesures nécessaires pour faire cesser l'atteinte à la vie privée. Le régime de la protection de la vie privée va permettre de combler les lacunes relatives au secret des correspondances, qui ne protège qu'une partie des données circulant sur le réseau. La vie privée étant une notion plus large, elle permettra d'élargir le champ d'application et de protection de la loi. Par conséquent, l'école ne pourra pas, sur son réseau, intercepter les informations qui touchent à la vie privée.
L'élève doit avoir la capacité de contrôler ce qui est fait des informations qui sont interceptées et qui le concernent, ainsi que de contrôler leur qualité. A vous d'en faire la demande à votre proviseur qui ne peut refuser.

LES PIRATES FONT DU RASE-MOTTES

Message 2 pour recherche portant sur **frequence patrouille de france**
De : bruboru (brubru@wanadoo.fr)
Objet :patrouille de france
Groupes de discussion :fr.rec.aviation
Date :2002-07-14 15:09:37 PST
View this article only

bout tous les pationner voici la frequence de la patrouille se matin a 9h50 en
direct

143.100 MHZ bonnee ecoute

Un message via un forum donnant la fréquence du jour de la PAF

ON SAVAIT CERTAINS PIRATES COMPLÈTEMENT IDIOTS, MAIS CEUX QUI ONT FRAPPÉ CET ÉTÉ DANS LE SUD DE LA FRANCE ONT TIRÉ LE POMPON DE LA BÊTISE HUMAINE. LE 12 JUIN 2003, UN PIRATE S'EST AMUSÉ AVEC LA FRÉQUENCE RADIO DE LA PATROUILLE DE FRANCE LORS D'UNE PRÉSENTATION. LE PROFESSIONNALISME DE NOS CHEVALIERS DU CIEL AURA PERMIS D'ÉVITER LE PIRE.

13 JUIN DANS LE CIEL DU PUY-DU-FOU

Comme chaque été, la Patrouille de France présente le fleuron de l'aviation militaire française. L'année 2003 étant d'autant plus importante pour nos "Top Gun" qu'ils soufflent la 50ème bougie de cette patrouille aérienne prestigieuse. Seulement, ce 13 juin n'est pas un jour comme les autres. La représentation des Alpha-jets va être interrompue en raison d'un problème de sécurité. Les pilotes et leurs machines qui survolaient le Puy-du-Fou, lors d'un spectacle de reconstitution historique, ont vu leur fréquence radio détournée. Les pirates se sont amusés à envoyer de fausses instructions de vol, qui à 850 kilomètres heure, auraient pu être catastrophiques pour les pilotes et le public venu nombreux.

PAPA, TANGO, CHARLIE

L'auteur de ce piratage est connu. Le journal local, Vendée matin, va d'ailleurs le confirmer dans son numéro 19649. Cependant, comment des avions militaires peuvent-ils être perturbés par un pirate en mal... de crash ? Le pirate serait-il un radio amateur inconscient ? Nous avons posé la question à plusieurs professionnels et radio amateurs éclairés. "Ce n'est pas vraiment un piratage", dixit le webmaster du site HELIMAT. "Dans les exhibitions en vol, une fréquence est attribuée au meeting. S'il est d'importance, par exemple au Bourget, il suffit de se reporter au Sup AIP sur le site de la DGAC, pour avoir les fréquences de trafic". (http://www.sia.aviation-civile.gouv.fr/, ndlr) A noter que si la représentation n'est pas "importante", c'est généralement la fréquence du terrain qui est prise en compte. "Bien souvent les militaires utilisent leur fréquence (qui ne figure pas sur les scanners, ni sur les radio d'aviation civile, ndlr) ce qui évite normalement ce genre de problème".

FOX TANGO

MINISTÈRE DE L'ÉQUIPEMENT, DES TRANSPORTS, DU LOGEMENT, DU TOURISME ET DE LA MER
DIRECTION GÉNÉRALE DE L'AVIATION CIVILE
DIRECTION DE LA NAVIGATION AÉRIENNE
SERVICE DE L'INFORMATION AERONAUTIQUE
6, AVENUE ROLAND GARROS - BP 245
F-33698 MÉRIGNAC CEDEX

SERVICE COMMERCIAL
☎ : 33 5 57 92 56 68
Fax : 33 5 57 92 56 69
✉ : sia-commercial@aviation-civile.gouv.fr
BNI
☎ : 33 5 57 92 57 92
Fax : 33 5 57 92 57 99
✉ : boi.sia@regis-dgac.net
AFTN : LFFAYNYX

AIP SUP 45/03
PUB : 08 MAI

LIEU : AD DE PARIS LE BOURGET, TMA PARIS

AIP SUP N° 45/03

1.3 Dispositions relatives au contrôle
1.3.1 Fréquences
Du 09 au 23 juin 2003 inclus, les aéronefs autorisés à utiliser l'aérodrome du Bourget doivent obligatoirement disposer, d'un ensemble émission réception VHF 760 canaux.
En plus des fréquences Air/Sol publiées pour Paris-Charles de Gaulle et Paris-Le Bourget, les fréquences supplémentaires ci-après sont exploitées : 135,700 « Le Bourget Hélicoptères », 129,475 (présentations en vol), 122,15 (préclairance), 127,350 (héliopérations) et 337,625 Mhz.

1.3.2 Dispositions particulières applicables aux avions
1.3.2.1 Plan de vol
Du 09 au 23 juin inclus, un PLN IFR ou VFR est obligatoire pour tout mouvement d'avion à destination ou au départ du Bourget ; en outre, pour les aéronefs participant à la manifestation, dans le champ 18 du PLN, il y a lieu de mentionner le code d'accès Salon communiqué par l'organisateur, en utilisant le format suivant : RPB/n° identifica-

Un document accessible sur Internet sur les fréquences aériennes.

Ecouter l'espace aérien est devenu un sport pour certains. Il suffit d'ailleurs de traîner un peu sur le réseau pour tomber sur de vrais fans. Un exemple, lu sur la liste fr.rec.aviation, où l'un des participants explique ce qu'il a pu "écouter" : " Contrôle : Fox Tango.... Vous avez quoi comme appareil ?... Le pilote : Ben... C'est la Patrouille de France au grand complet sur Alpha-jets qui aimerait très vite sortir des Cunimbs en verticale des Alpes". Nous nous sommes aussi rendus au pied de deux aéroports, Le Bourget et celui de Lesquin, dans le nord de la France. Nous avons pu y croiser des photographes à la recherche d'avions "rares" ou encore une fois, de grandes oreilles écoutant les pilotes conversant avec les tours de contrôle. L'usage et la détention d'une radio "aéro" est lié généralement à une licence. Couramment, des scanners sont achetés par quantité de personnes, mais ils n'émettent pas. Nous avons d'ailleurs été très étonnés durant notre reportage de la facilité d'achat d'un émetteur récepteur aéro (ICOM 3A ou autres modèles, ndlr). Une chose est sûre : il semble que pour ce 12 juin, la fréquence utilisée était locale et aurait pu coûter très cher.

LA LOI DES SÉRIES

Qui était donc visé par ce piratage ? Le Puy-du-Fou et son président Philippe de Villiers, ou la représentation militaire de la France représentée par la PAF ? Le plus terrible, c'est que le lendemain du piratage, la seconde démonstration aérienne sera annulée en raison... d'une panne radio. Les gendarmes mènent l'enquête. Pour le moment (du moins à l'heure où nous écrivons cet article, ndlr) le pirate n'a pas été trouvé. Les riverains font partie des témoins, car certains d'entre eux auraient entendu d'étranges messages diffusés par leurs postes de télévision.

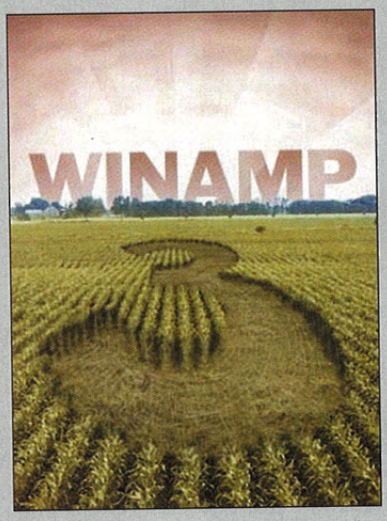
POUR EN SAVOIR PLUS, QUELQUES SITES À NE PAS RATER SUR :

La Patrouille de France
http://patrouilles.free.fr/
http://www.patrouilledefrance.com/

Sur les fréquences aériennes
http://www.fordyce.org/scanning/scanning_info/airshofq.html
http://neige.fleurb.jmsp.net/dossier/supaipmetro/SUP_2003_45_FR.pdf

SÉANCE À NET OUVERT

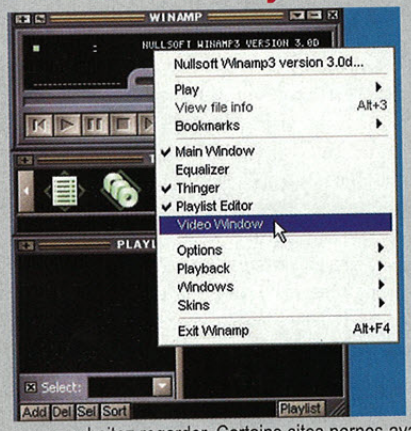
NOUS CONNAISSIONS LA DIFFUSION DE FILMS COMMERCIAUX PAR IRC, PAR LE PEER TO PEER, PAR LES FTP PIRATES... NOUS AVONS DÉCOUVERT QUE CERTAINS PIRATES AVAIENT TROUVÉ LE MOYEN DE DIFFUSER DES FILMS, DES DESSINS ANIMÉS, DES CONCERTSE VIA LES LOGICIELS DE STREAMING GRAND PUBLIC QUE NOUS AVONS TOUS DANS NOS MACHINES.



WIN !

Pour ceux qui ne connaissent pas encore Winamp, ce logiciel est LE lecteur multimédia par excellence. Il a été créé par la société Nullsoft en 1997. Ce fabuleux logiciel est capable de lire l'ensemble des formats audio et video numériques existants, dont le fameux format musical mp3. Sa légèreté et sa performance en ont fait son succès. Ce "player" est aussi capable de lire en "streaming", comprenez une lecture en live, en temps réel, un peu comme si vous écoutiez la radio sur internet. Winamp gère le streaming audio et... la diffusion des vidéos en temps réel.

DU WAREZ ? OÙ ÇA ?



Aussi étonnant que cela puisse paraître, il est possible d'accéder à une liste de serveurs diffusant des streaming video sur Winamp via quelques clics. Pour cela il suffit d'utiliser le menu déroulant "video", de sélectionner l'icône télévision, et une liste de serveurs streaming vidéo va se télécharger sur votre machine. Il ne reste plus qu'à sélectionner ce que vous souhaitez regarder. Certains sites pornos avaient déjà utilisé ce procédé pour attirer le "chaland" sur leurs sites. Aujourd'hui ce sont certains pirates qui s'organisent des séances publiques. Sur les 5 tests que nous avons pu effectuer, il nous avait été donné la possibilité de regarder Terminator 3, Tomb Raider 2, SWAT, le manga Trigun ou encore le cercle des gentlemen extraordinaires. Dans cette liste de serveurs il y a aussi bien le streaming de monsieur Dupont diffusé de son bureau, que d'autres fans de musique qui diffusent des clips en permanence ou des concerts.

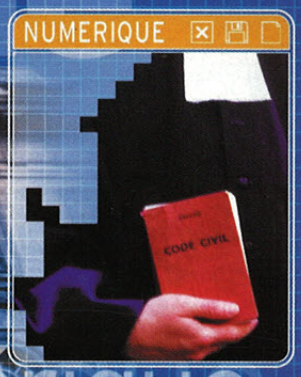
C'EST LÉGAL ?

Cette pratique est, vous vous en doutez, totalement illégale si la maison de production ne donne pas son accord pour la diffusion de ses oeuvres, et d'après ce que nous avons pu en voir, il y a peu de chances pour que ce soit le cas dans les vidéos qui étaient diffusées au moment de l'écriture de cet article. Cette pratique revient au même que diffuser des rip, des copies de dvd, les célèbres divx pirates via un site internet, ou des systèmes d'échanges de fichiers peer to peer comme KaZAa.

PROPRIÉTÉ INTELLECTUELLE

Cette méthode plutôt originale reste discrète et ridicule par rapport aux diffusions via le p2p. Mais rien ne pourrait empêcher de gros serveurs de streaming de se mettre en place pour diffuser des films à volonté. Ceux qui existent déjà ont de fortes chances d'aiguiser l'appétit des services juridiques des majors du disque et du film. Il faut rappeler que le piratage de logiciels, de musique ou de films, tombe sous le coup des lois régissant les droits de la propriété intellectuelle, les droits d'auteurs et la protection juridique des programmes d'ordinateurs. Les internautes outrepassant ces droits tombent sous le coup de la loi. Pour la France, nous vous invitons à lire ou relire les articles L.335-3, L.335-2 ou encore le L.122-4, qui stipulent noir sur blanc que " toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur est illicite " et que " la contrefaçon en France est punie de deux ans d'emprisonnement ainsi que de 150.000 euros d'amende ".

02/03 DECEMBRE 2003 - PARIS



1ER SALON JURIDIQUE DE L'internet ET DU numérique

CAP 15 - 75015 Paris/Organisé par les Éditions LEGITEAM en partenariat avec l'Observatoire APIPL

Prix d'entrée : 10 euros / Étudiants : 5 euros
Prix des colloques : 60 euros/colloque - Ateliers gratuits
Pass VIP : 300 euros/jour

Inscription obligatoire par mail, fax ou courrier : LEGITEAM
legiteam@free.fr - Tél : 01 49 10 38 73 - Fax : 01 49 10 38 94
17, rue de Seine - 92100 Boulogne-Billancourt

www.salonjuridique.com

Sous le patronage de
Madame Le Ministre Claudie HAIGNERÉ,
Ministre Déléguée à la recherche
et aux nouvelles technologies

Conseils juridiques
GRATUITS
sur place

TOP SPONSORS

CICERON · ECOSTAFF · Lamy · LRA Les Rencontres d'Affaires

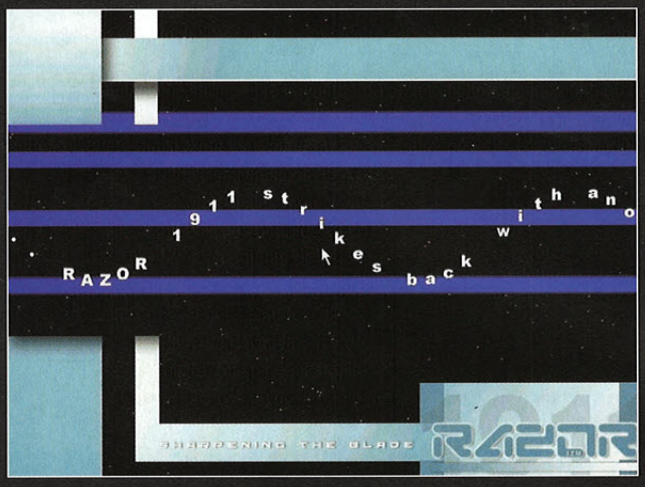
PARTENAIRES INSTITUTIONNELS : Chambre Nationale des Huissiers de Justice - ADEC

juriconnexion · CLUSIF · Conseil National des Barreaux CNB · cncpi · AFDIT · GESICA Assistance · Chambre des Notaires de Paris Seine-Saint-Denis/Val-de-Marne

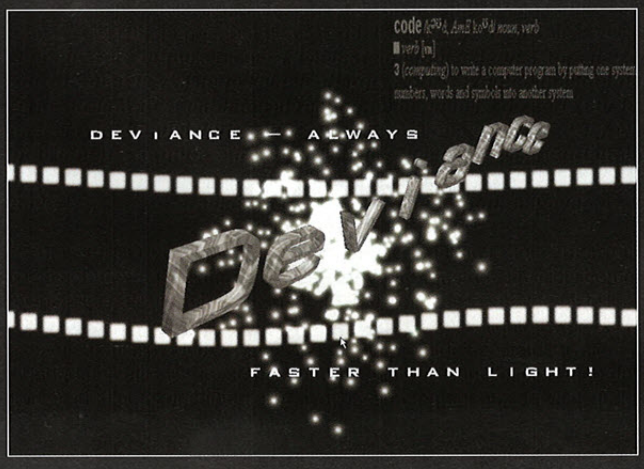
CRACK AND CRASH

Sur le web on trouve de tout. Les amateurs de logiciels y trouvent aussi les outils qui permettent de faire une copie de sauvegarde en bonne et due forme de leurs logiciels achetés en magasin. Comment est-ce possible ? Comment ça marche ? Est-ce vraiment légal ? Découverte de ces pages web qui "crackent" pour vous. On en profite aussi pour passer du côté de ces sites qui vous font gagner dans tous vos jeux.

CRACK, KESAKO ?



Le mot crack vient de cracker, casser. A la base, un cracker est un logiciel, et aussi son utilisateur, qui aura pour mission de casser un mot de passe, une protection. Le logiciel de crack peut, par exemple, égrainer des mots de passe jusqu'à ce qu'il en trouve un qui soit valide. Le plus connu de ces programmes se nomme crackjack. Sur le web on trouve aussi des cracks, de petits programmes qui permettent de faire sauter des protections de logiciels. Ils fonctionnent simplement, ou presque. Vous copiez votre original. La copie ne fonctionne pas en raison de la protection. Le crack va permettre le bon fonctionnement de cette copie de sauvegarde. L'utilisation d'un crack n'a rien d'illégal si vous avez acheté l'original. La mise à disposition de cette copie de sauvegarde à une tierce personne, est quant à elle, totalement illégale et sévèrement punie. Cependant, un bémol : la modification d'un software est aujourd'hui quasiment interdite par tous les éditeurs, du moins sur le papier, et en lisant les notices d'utilisation vous verrez certains avertissements sans fioritures.



MOT DE PASSE, TIMER...

Les protections placées dans les logiciels sont variées. Il y a l'anti-piratage simple, qui bug la copie effectuée. La protection par mot de passe, qui oblige à entrer un ou plusieurs sésames afin de pouvoir utiliser son produit. Qui n'a jamais ragé après avoir perdu ou jeté cette satanée boîte ou notice où était notifié le mot de passe ? D'autres protections utilisent le temps. Vous pouvez utiliser un logiciel durant une certaine période. D'autres bloquent des options du logiciel. Dans ces deux derniers cas, les protections sont utilisées pour les shareware. Les auteurs de ces cracks trouvent l'astuce pour passer ces sécurités. Ils jouent, soit avec la base de registre, ou soit dans la plupart des cas, avec la partie du code du logiciel qu'ils souhaitent cracker.

SHOOT AND GO !

Des dizaines de sites sur la toile proposent ce genre d'outils. En voici une petite sélection. Attention ! Pour télécharger ce genre de choses vous devez être en possession de votre original et d'un bon antivirus. Il n'est pas rare de voir les "cracks" être agrémentés de virii ou de chevaux de Troie afin d'espionner les utilisateurs.

TRAQUE SUR INTERNET

Alors que l'utilisation d'un crack sur ses propres logiciels n'est pas une fraude en soi, beaucoup de sociétés mettent en place des systèmes de protection qui épient les utilisateurs qui pourraient se transformer en pirates.

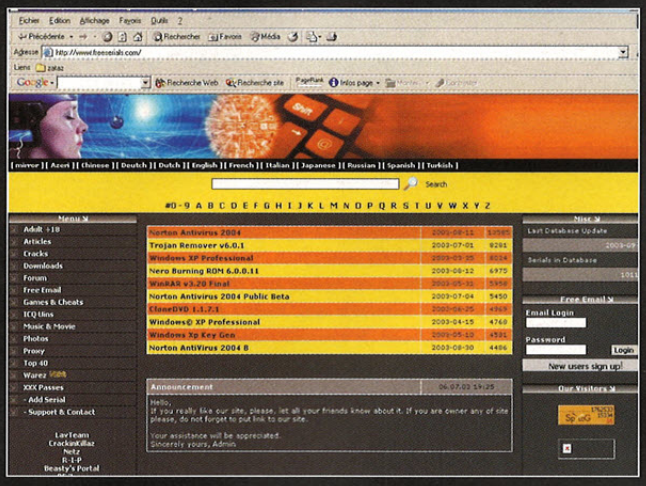
Plusieurs lecteurs nous ont fait part d'une forme d'espionnage qui a pour but de protéger les logiciels des pirates. Voici l'un des mels reçus : ***"J'ai testé un logiciel qui s'appelle zéro popup killer, je l'ai téléchargé. Pour savoir ce que donnait la version complète j'ai recherché le numéro de série sur le web et je l'ai entré pour avoir la version complète. J'ai reçu un mel sur mon adresse officielle - que je n'avais pourtant pas donnée - de cette société, m'avertissant que j'utilisais un programme "cracké" et que j'avais 5 jours pour le payer"***.

Ce genre de méthode est illégal en France, mais utiliser un logiciel piraté l'est aussi. A noter que des logiciels comme FlashFXP contrôlent chaque 1er du mois si la version installée sur un PC est achetée ou non. Nous vous expliquions, en exclusivité dans ZATAZ Magazine 3, comment des sociétés avaient mis en place des systèmes anti-piratage utilisant l'espionnage des utilisateurs via des mels envoyés directement aux services juridiques des sociétés copiées.

SERIAL SITE

Ce site propose des cracks, plus de 16 000, des serials, les fameux numéros de série.
http://www.serialsite.com/

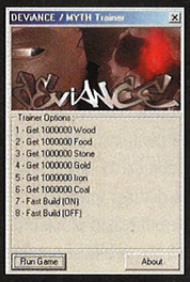
FREE SERIAL



Plus de 101 135 cracks, serials. Propose des logiciels permettant de contourner certaines protections pour jeux de consoles de jeux.
http://www.freeserials.com/

MOTEUR DE RECHERCHE

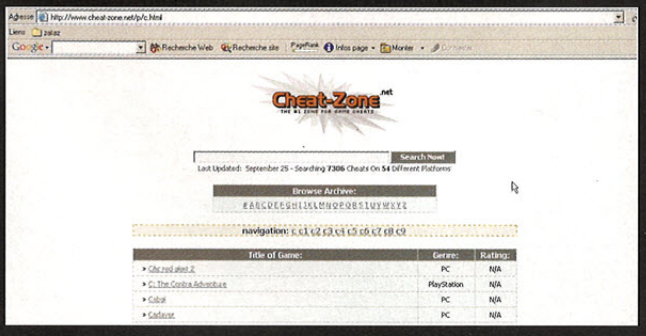
Ce portail propose pas moins de 140 sites dédiés uniquement aux cracks et aux serials. Certaines pages proposées ne sont rien d'autre que des sites pornos. Prudence donc. http://allseek.info/



CHEAT OR TRAINERS

Qui n'a jamais ragé de ne pas pouvoir passer un niveau trop difficile dans un jeu ? Avoir de l'énergie infinie pour blaster tous ces aliens du level 50 ou récupérer toutes les clés, d'un coup, pour continuer sa quête ? Les cheats mode et trainers sont là pour vous y aider. Voici une sélection de sites qui vont vous faire gagner à tous les coups.

CHEAT ZONE



Sobre mais efficace. Cheat Zone propose des codes pour gagner, avoir de l'argent, être invincible sur tous les supports pouvant permettre de jouer. On a pu y voir aussi les premiers cheats mode pour jeux, dédiés aux téléphones portables. http://www.cheat-zone.net

CAMARADE

Le site cheats, avec sa belle extension en ru (comprenez Russie), propose quelque 100 000 trainers, cheats mode... pour toutes les machines et consoles.
http://cheats.ru/

ARE YOU READY ? (IMAGE : ALLSEEK.JPG)

D'entrée de jeu, le site annonce 200 000 cheats mode et trainers.
On veut bien le croire, vu qu'il propose des moyens de tricher dans un jeu sur 31 machines, allant de la console de jeu 3Do à la XBox en passant par la Gameboy Advance de Nintendo ou encore la GP32. Seul inconvénient : le site pullule de publicité pour des sites pour adultes.
http://www.allyourcheats.com/

AUTRES

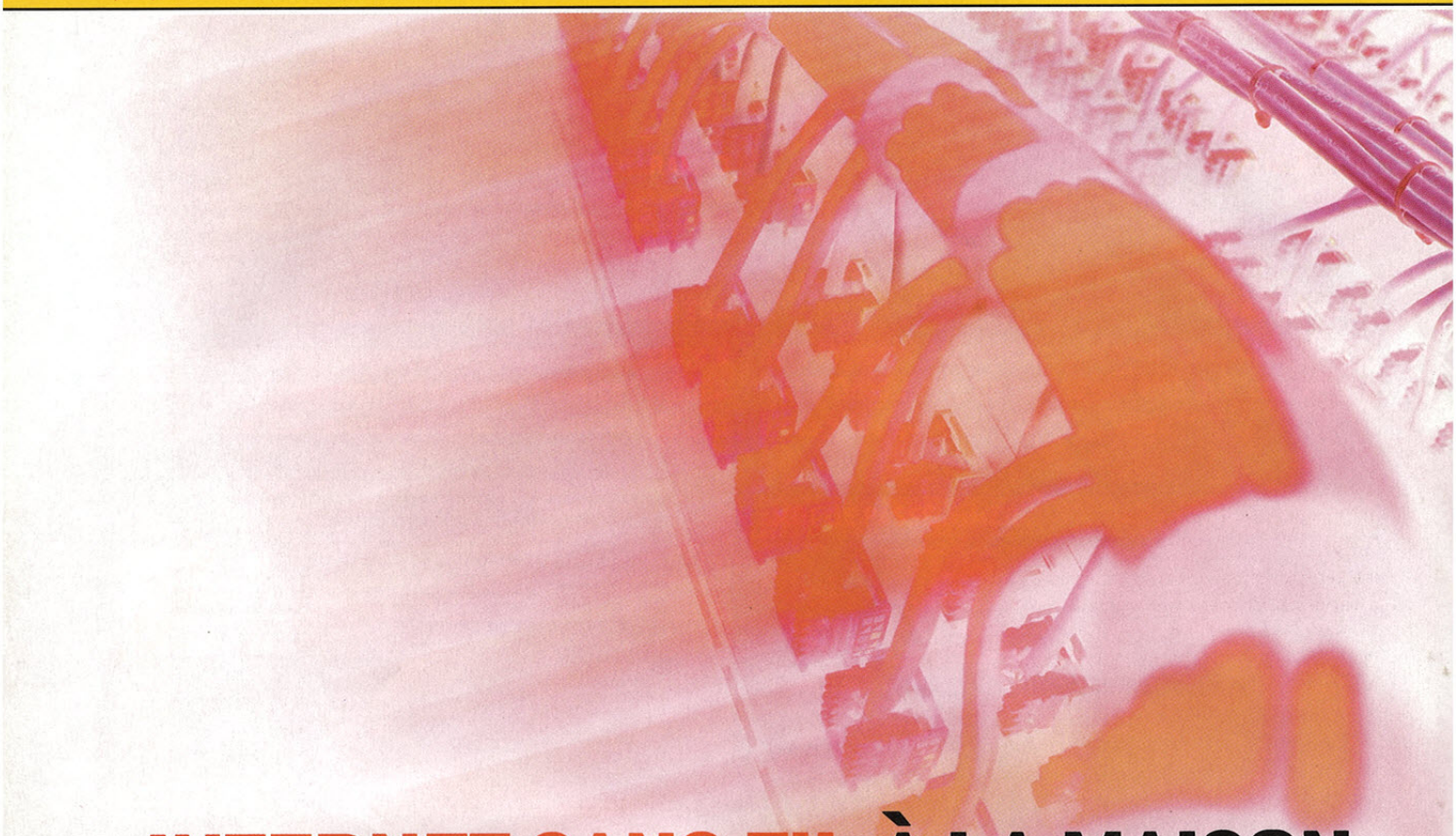
http://www.cheats.it/
http://www.cheatportal.dk/
http://www.cheathappens.com/
http://www.cerials.net/
http://www.trainerscity.com/
http://www.codycheaty.com/

WING OF DEATH

Le problème des cracks, c'est qu'ils servent aussi à pirater des logiciels. Ne nous voilons pas la face : l'honnêteté intellectuelle de certains internautes dépasse l'outil qui doit permettre d'aider à la copie de sauvegarde.

Des sociétés comme DELL en ont fait les frais. Dell Inc a dû enlever de son site internet le logiciel Axim pour Pocket PC 2003 après que des pirates aient cracké le logiciel en question pour "releaser" une copie de cet OS.

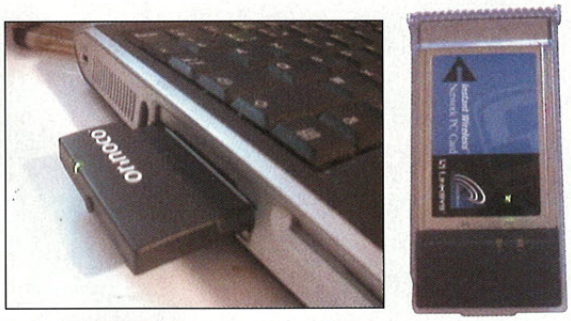
La demande de téléchargement a été telle, après la sortie du crack, que DELL a été obligé de retirer l'OS de son site.



INTERNET SANS FIL À LA MAISON

Avec les fêtes de fin d'année qui arrivent à grands pas, peut-être allez-vous faire une liste au papa Noël spéciale informatique cette année. Ca tombe bien, nous aussi ! Si vous êtes comme nous, on va se lancer dans le wi-fi dans notre quartier :) Voici donc les trucs et astuces à connaître pour avoir un réseau sans fil digne de ce nom.

Adaptateur/émetteur

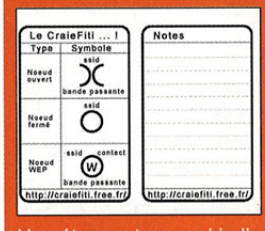


Carte PCMCIA permet de mettre en réseau un portable.

QUE CHOISIR ?

Il existe aujourd'hui plusieurs technologies sans fil. On y trouve l'UMTS, le Bluetooth, et bien sûr le wi-fi. L'UMTS diffuse sur plusieurs centaines de mètres à un débit de 1 Mega bits seconde. Le wi-fi a un débit de 11 Mega bits seconde, mais il a un petit défaut : son antenne permet de diffuser internet, mais plein d'autres choses aussi, sur une dizaine de mètres. Il existe plusieurs versions : le 808.11b, le 802.11g qui permet un débit de 54 Mega bits seconde. Pour être plus précis, le standard 802.11 technique est défini par l'IEEE, Institute of Electrical and Electronical Engineering. Il travaille dans une bande

LE CRAIEFITI



La mode a commencé en Australie, où certains murs arboraient cet étrange signe cabalistique.

Aujourd'hui, ce signe est apparu en Angleterre, en Allemagne et en France. Des marques, nommées "war chalkers" laissées par les amateurs "underground" des réseaux sans fil. Une étrange trace qui indique que le lieu est propice à l'interception de connexions sans fil... appartenant à des entreprises.

De l'Internet gratuit sur le dos de sociétés qui paient la bande passante, mais heureusement pas tout le temps.

http://www.zataz.com/zatazv7/news.php?id=1183

de fréquences radio de 2,4 gigahertz. D'ici quelques années (on parle de 2006/2007), le standard devrait passer au 802.11 avec un débit qui fait rêver, qui est de 108 Mega bits seconde sur des fréquences de 2,4 et 5,2 gigahertz.

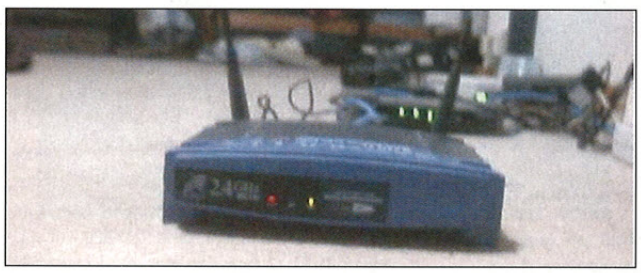
ANTENNES ET LOGICIELS

http://www.freeradius.org
http://seattlewireless.net/?BuildingYagiAntennas
http://www.wireless-fr.org/contributions/antenne-yagi/Antenne-directionnelle.html
http://www.xaviervl.com/Antenne/
http://reseaucitoyen.be/index.php?AspectsAntennes
http://cbonnan.free.fr/site-wifi/antennes/antennes.html
http://clorenz.free.fr/
http://www.jm-music.de/projects.html

SÉCURISATION

Le problème du wi-fi, c'est sa sécurité. Les défaillances des outils de sécurité intégrés, comme le codage WEP, comprenez Wired Equivalent Privacy, oblige à mettre en place des moyens plus sérieux pour éviter de voir un petit curieux visiter votre machine et pire, utiliser votre connexion à des fins criminelles. Première chose : la "wi-fi Alliance", géniteur du label wi-fi, explique que le standard TKIP, la Temporary Key Integrity Protocol, est une obligation. La norme 802.11i intègre ce cryptage temporaire TKIP. Baptisée CBC-MAC Protocol, cette encryption se base sur le célèbre AES, l'Advanced Encryption Standard. Un chiffrement symétrique à 128 bits. Voici quelques mesures obligatoires à prendre lors de la mise en place de votre réseau.

- **Ne pas hésiter à changer régulièrement de clé WEP.** Mot de passe fort, évitez le nom de famille indiqué sur la sonnette de la maison. Nous avons vécu des cas pathétiques dans ce genre d'erreur.
- **Protéger les postes clients indépendamment du réseau.**
- **Empêcher les connexions anonymes.**
- **Placer votre antenne loin des murs et des fenêtres.** Le centre de votre maison est le meilleur emplacement. La diffusion sera moindre. Utiliser des logiciels comme Netstumbler pour PC et iStumbler pour Macintosh pour établir la carte précise d'émission de votre réseau.
- **Ne pas oublier de changer les mots de passe** que peut proposer le matériel. Les passwords mis en place à l'usine doivent être modifiés.
- **Utiliser des logiciels comme NetStumbler** pour contrôler les connexions autorisées ou non (Logiciels sur le CDrom). D'autres contrôleurs d'accès existent, comme ceux de Nomadix ou encore ReefEdge.
- **Modifier le SSIDS, les identifications de votre matériel.** N'utiliser aucun nom évident comme votre adresse ou votre nom de famille. Des logiciels comme Kismet sont capables de sniffer, de repérer ce genre d'information.
- **Contrôler les IP de connexion à votre réseau.** Seuls les accès autorisés peuvent entrer.
- **Si vous vous faites votre réseau personnel, limitez le nombre de connexions à une personne :** vous.
- **Installer un firewall** qui soutient la connectivité VPN.
- **Ne pas hésiter à faire appel à des passionnés et des professionnels** dans le cas d'une mise en réseau pour entreprise. Vous trouverez un grand nombre d'articles sur la sécurité des réseaux sans fil sur le site airdefense.net.



AP. Indispensable pour partager un accès ADSL.

LE MATOS ET LES LOGICIELS

Pour vous connecter, il va vous falloir un routeur. Les prix varient entre 100 et 400 euros. Le routeur se connecte directement au modem haut débit. Certains routeurs font aussi office de modem, en port Ethernet ou USB. Dans le second cas votre réseau doit rester allumé pour se connecter. Aux utilisateurs d'un ordinateur portable, il faut un adaptateur wi-fi. L'antenne est intégrée, certaines autres cartes préfèrent la jouer martien avec un gros morceau de caoutchouc qui dépasse. Comptez entre 50 et 80 euros. Il existe le même genre de matériel pour les PALM et autres Pocket PC. Les cartes sont des Compact Flash. Entre 100 et 190 euros. Voici une liste - non exhaustive - de logiciels utilitaires qui vous permettront d'utiliser d'une façon optimale votre réseau wi-fi, voire celui du voisin, tout en sachant que toute intrusion et maintien dans un système d'information est durement réprimé par la loi française.

AIRSNORT: SNIFFER ET CRACKER WEP 802.11B

Airnsort est un outil WLAN qui permet de découvrir les clés de cryptage WEP. Airsnort analyse passivement les transmissions WLAN et permet de cracker les encryptages WEP dès qu'il a capturé un nombre de paquets nécessaire. Vous pourrez aussi récupérer les SSID des réseaux WLAN et voir si un réseau est protégé par WEP. Airsnort a besoin approximativement de 5 à 10 millions de paquets encryptés pour pouvoir deviner une clé WEP.
Deux types de chipset sont supportés par Airsnort, les chipsets Prism2 (wlan-ng) et Orinoco (orinoco-cs).

LES INDISPENSABLES

http://www.wifi-vitry.net/
http://wiki.rennes-wireless.org/
http://www.wifi-montauban.net/
http://craiefiti.free.fr/
http://www.wlanfr.net/forum.php?op=forum&pid=13
http://www.nantes-wireless.org/
http://w4-web129.nordnet.fr/forum/
http://www.mobilenetswitch.com/

SPOTS FRANÇAIS

Quelques spots français que nous avons pu tester.

38 Grenoble : ESC Grenoble. Ecole de Management. Hôtel d'Angleterre.

49 Cholet : Pub du Cadran.

51 Reims : ESC Reims.

59 Lille : ESC Lille - Rédaction ZATAZ - du côté de la place Rihour.

64 Pau : Hôtel Roncevaux - Centre de Congrès.

67 Strasbourg : Centre de Conférences.

86 Poitiers : Ecole Supérieure de Commerce et de Management.

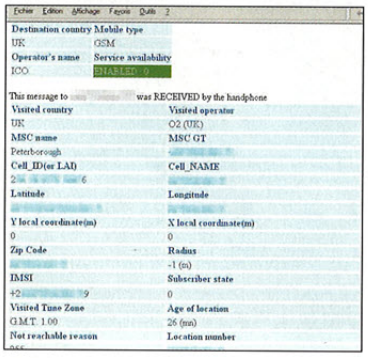
75 Paris : Gare du nord - Bercy - Sofitel (12e arr). Restaurant Les Cailloux (13e)

TRACER GSM

Comment "localiser", partout dans le monde, une personne qui possède un GSM ? ZATAZ Magazine l'a trouvé grâce à une simple connexion internet. Nous avons découvert que des sociétés sur le web, mal protégées, permettaient ce genre de chose. Découverte ZATAZ Magazine.

SPY TO LOVE ME

Alors que nous recherchions une information pour notre hors série GSM - en kiosque en ce moment, nous sommes tombés sur une société pas comme les autres. Nous ne donnerons pas son nom ici, mais sachez qu'il s'agit d'un spécialiste du routage international de SMS qui propose un service d'interconnexion de SMS aux opérateurs. Une interconnexion qui permet d'envoyer et de recevoir des SMS dans n'importe quel pays du globe. Cette entreprise est raccordée à la passerelle SS7 international. Une passerelle qui permet l'interfonctionnement entre les réseaux IP et le réseau public de téléphonie, qui traite plus de 20 millions de SMS mensuellement et qui est active sur plus de 600 réseaux de téléphonie mobile dans le monde. Cette société a, caché sur son serveur mais pourtant accessible via plusieurs mots clés Google, un service d'espionnage de GSM. Avec un simple numéro, celui de votre petit(e) ami(e) par exemple, vous seriez capable de connaître la situation géographique de ce(tte) dernier(e) en lui envoyant un simple SMS.



Destination country	Mobile type
UK	GSM
Operator's name	Service availability
ICO	ENABLED: 0
This message to [redacted]	was RECEIVED by the handphone
Visited country	Visited operator
UK	O2 (UK)
MSC name	MSC GT
Peterborough	[redacted]
Cell_ID(or LAI)	Cell_NAME
2[redacted]6	[redacted]
Latitude	Longitude
[redacted]	[redacted]
Y local coordinate(m)	X local coordinate(m)
0	0
Zip Code	Radius
[redacted]	-1 (m)
IMSI	Subscriber state
+2[redacted]9	0
Visited Time Zone	Age of location
G.M.T. 1.00	26 (mn)
Not reachable reason	Location number

COMMENT EST-CE POSSIBLE ?

SMS, le célèbre Short Message Service, est un service qui permet d'envoyer ou de recevoir de courts messages textuels via votre mobile. Le site officiel de la société propose un service d'envoi de SMS à travers le

Les informations sur le positionnement du GSM du rédacteur en chef de ZATAZ

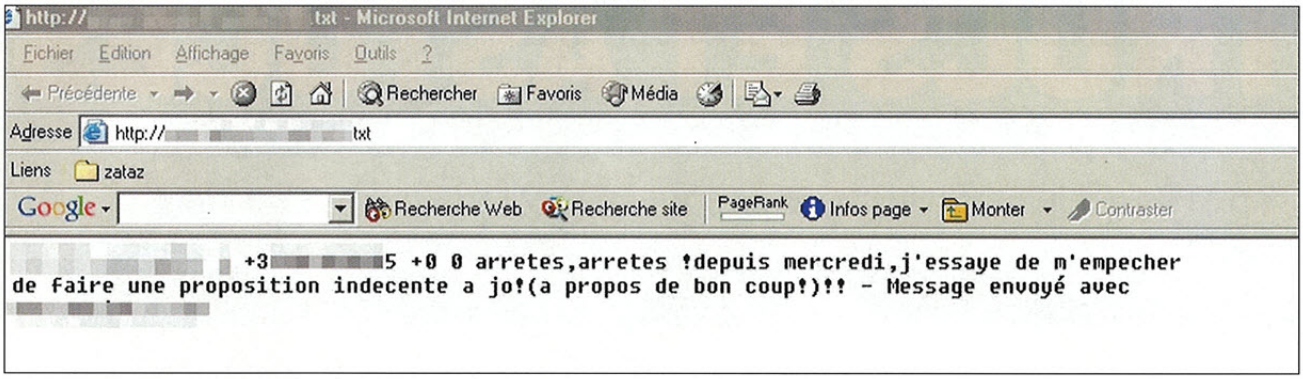
UN BUSINESS... JUTEUX

Nous vous avions déjà parlé de ce genre de localisation voilà un an. Une société britannique, nommée MapAMobile, propose, pour 70 centimes d'euro, de tracer n'importe quel téléphone mobile.

Pour le moment ça fonctionne avec les abonnés britanniques. Le système reste classique : triangulation via plusieurs antennes de relais. MapAMobile annonce le traçage d'un GSM à 40 mètres près.

Dans le même genre de " produit ", la société Tiger Télématique propose de suivre à la trace les petits britanniques possesseurs d'un téléphone mobile. On connaissait déjà la puce à implanter dans le bras, voici donc le traceur dans le GSM.

Le dispositif doit permettre aux parents de suivre leurs enfants via un site internet, "Notre système est capable de définir l'emplacement d'une personne à 10 mètres près." Dixit Geoff Mitchell, le directeur général de Tiger Télématique.



monde via une simple page. La fonction de celle-ci est d'envoyer un SMS et d'indiquer la position du destinataire. A noter d'ailleurs que nous avons été capables de trouver, toujours par Google, les logs des messages envoyés par SMS, ainsi qu'une liste de numéros de téléphone à faire frémir un télémarketer.

TECHNIQUEMENT

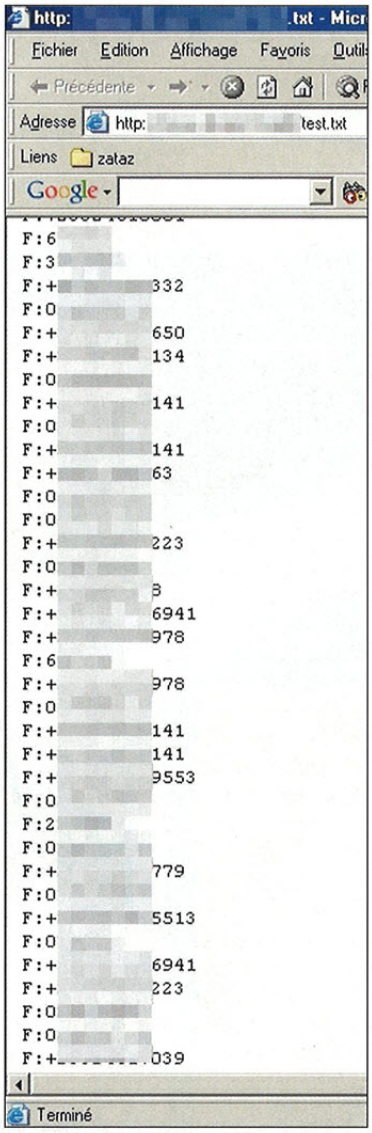
Le système GSM a ceci de particulier qu'il inclut un réseau, c'est-à-dire que tous les opérateurs sont reliés entre eux ; cela s'appelle le SS7 (signaling system 7). Ceci autorise n'importe quel utilisateur à aller à l'étranger et à facilement téléphoner avec son propre téléphone, si des accords ont été passés avec les opérateurs étrangers.

Maintenant, nous allons détailler le système et plus particulièrement les envois des SMS, puis montrer comment ce merveilleux réseau SS7 permet de localiser tout un chacun. Parlons concret, imaginons un utilisateur de la compagnie ZATAZ Telecom, situé 10 rue des huîtres à Paris dans le 10ème arrondissement.

Cet utilisateur est sous la couverture d'une cellule (les antennes plates que vous voyez sur les toits : ce sont des cellules, ndlr), cette cellule fait partie d'une zone de plusieurs cellules, dont l'ensemble est géré par un MSC, le " chef " de ce groupe de cellules, qui sait tout ce qui s'y passe. Comme le réseau de ZATAZ Telecom est très grand, il a plusieurs MSC. Cet ensemble de MSC est géré par un HLR, comprenez un Home Location Register.

C'est ce HLR qui sait tout ou presque. C'est une sorte de grosse base de données où se trouvent toutes les données de l'abonné : son numéro de téléphone, dans quel MSC il est actuellement enregistré, s'il a le droit de faire telle ou telle chose qu'autorise son abonnement... Maintenant, imaginons une compagnie nommée : MECHANTS Telecom. Cette dernière veut envoyer un SMS. Cela se passe en 2 temps.

D'abord M.T. envoie la requête SRI, Send Request Info. Pour simplifier, elle contacte le HLR de l'opérateur en lui demandant de trouver le téléphone cible. Le HLR répond à MECHANT Telecom et donne des informations. La principale étant le MSC auquel est actuellement rattaché le téléphone.
Une fois que M.T. a eu cette information, elle contacte le MSC pour envoyer le message. Le MSC renvoie le CellID, l'identifiant de la cellule auquel est rattaché le téléphone, et M.T. peut enfin envoyer le message. (Image : trace3.jpg – Légende : ici, un log d'un MSN stocké sur un serveur web.)



Légende : ici, un log d'un MSN stocké sur un serveur web.

Il faut savoir que les opérateurs s'échangent entre eux des documents appelés IR21, dans lesquels des centaines d'informations sont présentes, comme la liste des HLR et leurs emplacements. Dans de grandes villes telles que Paris il y a plusieurs MSC, et le fait de savoir à quel MSC est rattaché le téléphone nous permet donc déjà de savoir, avec une précision variable, où est l'utilisateur.

Ensuite, quand un message est envoyé, le MSC communique le CellID ; il est théoriquement possible à n'importe quelle compagnie ayant un accès SS7 de savoir à quelle antenne est rattaché le numéro de téléphone... De plus il y a généralement 3 antennes par cellule. Trois antennes plates, émettant à 120 degrés, ce qui donne une couverture à 360 degrés. Généralement les opérateurs respectent un processus : l'antenne numéro 1 se trouve toujours au nord. La seconde au sud ouest, etc... On peut donc même savoir si vous êtes au nord ou au sud de l'antenne via une triangulation.

Avec des sites tels que ARCX - http://www.arcx.com/sites/MicrocellCIDOttawa.htm - on peut facilement monter une base de données reliant les CellID avec l'emplacement réel de la cellule, même si nous ne sommes pas l'opérateur. L'opérateur sait, bien sûr, exactement où vous êtes… Cela est nécessaire, sinon on ne pourrait pas vous téléphoner ni vous envoyer de SMS.

TRUCS ET ASTUCES

**Suite de notre article sur le Buffer Overflow.
Dans ce numéro, comment protéger les logiciels des pirates.
Autre astuce, comment cracker les mots de passe encryptés en md5.**

CASSER UN MOT DE PASSE ENCRYPTÉ EN MD5

Nathaniel vous propose un code pour casser le md5, un algorithme d'encryption. Vu que l'on ne connaît pas actuellement la clé qui permet de décrypter un fichier codé en md5, nous vous invitons à vous munir d'une bonne wordlist, un dictionnaire de mots, et du petit script que vous trouverez sur votre CDrom.

On sait que dans le langage php il est possible d'encrypter un fichier en md5 via la commande md5(fichier). On ne peut pas le décrypter. Nathaniel a trouvé une solution. Encrypter un par un chaque mot d'une wordlist jusqu'à ce que le résultat crypté de l'un des mots de cette liste soit égal à notre pass à décrypter. Voici le code source commenté pour mieux cerner le problème. Ce code est à entrer dans une page html qui appelle le cracker, **brutus.php.**

```
<!-- Code html -->
<html>
<!-- Début du form -->
<center><big>.:: Brutus pwd MD5 By Linux ::.</big></Center><br><br>
<br><br>
<FORM METHOD="POST" ACTION="brutus.php">
<CENTER>
<!-- Une textbox qui s'appelle "decrypt" -->

Pass a décrypter :  
<INPUT TYPE="text" NAME="decrypt">
<BR><BR>
<!—Le bouton " start " qui a comme fonction d'appeler l'action "brutus.php" --
>
<INPUT class="button" type="submit" name="Envoyer" value="START">
</CENTER>
</FORM>
</BODY>
<!-- Fin du Code html -->
</HTML>

<?php
{echo("Brutus PWD MD5 V1.0 By Linux (EvilNux) ON ..");} //Le programme
fonctionne.
$Fichier = fopen("Wlist.txt", "r"); //Open -- Ouvre un fichier txt en mode lectu-
re, le fichier ici c'est Wlist.txt
                                    // Le nom "technique" de ce fichier est
$Fichier (variable)
$Contenu_fichier = fgets($Fichier); //Get -- Récupère les données du fichier
qui étaient dans $Fichier
                                    // L'ensemble des infos dans la
variable appelée $contenu_Fichier
fclose($Fichier); //close -- On ferme le fichier ($fichier)
$Ligne = array(); //Création d'un tableau
$Ligne = explode("\n", $Contenu_fichier); //Inserer la variable
$Contenu_Fichier (Décomposition en lignes)
for ($nb = 0; $nb < sizeof($Ligne); $nb++)  //Le nombre de lignes n'est pas
atteint, la boucle continue.
$nb = $nb + 1;                      //A chaque retour de la boucle $nb = $nb + 1
$password = Ligne[$nb];
$passcrypted = md5($password);  //Encrypte en md5 - $password =
Ligne[$nb]
if ($passcrypted == $_POST["decrypt"])
{echo($password);break;} //on affiche le password d'origine et la boucle stop
(break)
else
{echo("Mauvais passe.");} //Erreur et la boucle continue
}
?>
```

LES BUFFERS OVERFLOW - PARTIE 2

Dans le 9e numéro de ZATAZ Magazine nous vous faisions découvrir le fonctionnement du buffer overflow. Le but ce mois-ci est d'apprendre à déceler les vulnérabilités et à les corriger. Nous allons donc examiner les fonctions à risque et découvrir leurs équivalents sécurisés ainsi que quelques principes de base.

Voici rapidement le principe du dépassement de tampon (nom français du buffer overflow, ndlr).

Certaines fonctions utilisées en programmation ne contrôlent pas la quantité de données que l'utilisateur leur transmet.
Résultat : si on met trop de données, ça déborde !
Et ce débordement permet dans certains cas de prendre le contrôle partiel ou total de la machine sur laquelle il est exécuté : c'est la faille du buffer overflow.

Pour éviter ces problèmes, il est important que le programmeur vérifie pour chaque valeur qui sera entrée par l'utilisateur, dans quelle variable elle sera stockée, et surtout qu'il utilise des fonctions sécurisées. Il est également possible de prévoir une petite marge ; par exemple pour un numéro de téléphone, prévoir la place pour 12 chiffres au lieu de 10.

Voyons maintenant quelques programmes vulnérables et comment les sécuriser :

```
#include <stdio.h>
int main(int argc, char **argv)
{
char buffer[10];
strcpy (buffer, argv[1]);
}
```

Le programme copie le contenu du premier argument passé par la ligne de commande (lorsque vous tapez : c:\vulnerable.exe larsus alors le mot "larsus" est appelé premier argument) dans la variable buffer.

Le problème se situe au niveau de la fonction strcpy qui ne vérifie pas que cet argument contienne bien 10 caractères au maximum (taille du buffer). Pour résoudre ce problème il faut utiliser la fonction strncpy et lui indiquer de ne copier que 10 caractères : strncpy (buffer, argv[1], 10); et voilà le problème corrigé !
// Tu avais indiqué strcpy(buffer, argv[1], 10) ; j'ai supposé que c'était strncpy (...) , si pas bon remets comme avt :p

Une autre fonction posant des problèmes est strcat. Elle a pour effet de copier la deuxième variable que le programme lui donne à la suite de la première, mais comme strcpy elle n'effectue aucun contrôle sur ce qu'elle fait. Voici un exemple ([...] représente une partie de programme sans importance) :

```
#include <stdio.h>
int main(int argc, char **argv)
{
char nom[20];
char prenom[20];
[...]
strcat (nom, prenom);
}
```

Analysons le programme : nous avons un nom de 20 caractères maximum et un prénom formé également de 20 caractères maximum. Ensuite le prénom est mis à la suite du nom grâce à strcat. Pas de soucis, mais seulement en apparence, car si le nom est suivi du prénom cela donne 40 caractères dans l'emplacement nom limité... à 20 caractères !
Il faut donc utiliser la fonction strncat:
strncat (nom, prenom, 20);

Ces exemples sont certes très simples, mais on les rencontre trop souvent chez les programmeurs débutants et dans une bonne partie des programmes commercialisés ! Voici un cas de figure plus compliqué :

```
#include <stdio.h>
int main(int argc, char **argv)
{
char nom[30];
FILE *fichier;
fichier = fopen("x-ray.txt", "r");
fread (nom, sizeof(char), 1024, fichier);
}
```

Le programme crée une variable nom de 30 caractères
et ouvre le fichier **x-ray.txt**.

Le problème intervient à l'appel de la fonction fread. En effet, on lui demande de lire 1024 octets, c'est-à-dire 1 ligne dans le fichier texte, et de copier cela dans la variable nom. Si on admet que le nom fait moins de 30 caractères. Mais si jamais celui-ci est plus long, il y a là une faille potentielle. Il faut donc faire attention à remplacer 1024 par 30 pour ne pas lire toute la ligne contenant le nom, mais seulement les 30 premiers caractères.

DÉCRYPTAGE FLASH

C'est début septembre 2003 que la team française Alex-Family décide encore de faire parler d'elle en sortant un nouvel outil permettant de décrypter n'importe quel fichier du logiciel FlashFXP. Nous avons cherché comment ceci était possible. Installez-vous confortablement dans votre fauteuil, car ça va décrypter dans les chaumières.

UN PROBLÈME PAS HABITUEL

On peut dire que les exploits permettant de contourner les protections des logiciels ne se font pas rares sur internet. De nombreux sites les recensent dans de gigantesques bases de données permettant à tout débutant de se prendre pour un cracker d'un jour, en 'oubliant' de payer ses licences d'utilisation.
FlashFXP est sans doute le plus utilisé des logiciels de transfert de fichiers (ftp) sous Windows. Il a lui aussi déjà subi le sort des crackers qui ont sorti divers patches pour détourner la protection de ce shareware à 25 $.

Mais le problème mis en évidence dans cet article est bien différent, et sans doute beaucoup plus dangereux. En effet, les hackers ne se sont pas seulement concentrés sur la protection du shareware, mais aussi sur la protection des données sauvegardées par ce dernier.
Ils ont alors découvert comment étaient stockées et cryptées les informations concernant les serveurs ftp, les mots de passe, les noms d'utilisateurs et les ports enregistrés via le 'Site Manager' du logiciel.

TROP FACILE ?

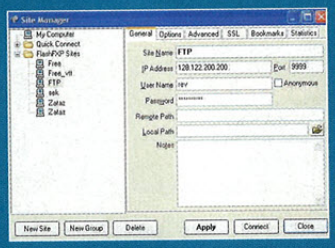
N'importe quelle personne ayant accès d'une façon ou d'une autre à un poste où est installée une version de FlashFXP sera dorénavant en mesure de décrypter tous les accès ftp des utilisateurs du logiciel. Les hébergements Web, les ftp les plus sécurisés, ou même les accès aux stro warez tomberont alors aux mains du moindre script kiddies.

POURQUOI ALORS DÉVELOPPER UN OUTIL SI FACILEMENT UTILISABLE ?

Interrogé, Alex-Ploit, membre créateur de la team française, nous répond : " Nous avons développé cet outil en ligne dans le but de montrer l'importance de la faille et d'expliquer comment s'en protéger. Peu de personnes prennent en effet les problèmes de sécurité au sérieux. Par cette démonstration impressionnante, les utilisateurs prendront le temps d'y réfléchir ... "

LE PROBLÈME

Selon CEDSoft, la société éditrice, FlashFXP n'a jamais souhaité rendre la protection de ces données inviolables. "The scheme used for site passwords was never intended to resist an attack where the attacker reverse engineered our encryption algorithm." En effet, le procédé de décryptage est très simple et ne nécessite que très peu de calculs. Il est donc facile de produire des outils qui automatisent le procédé et qui donnent le résultat très rapidement, tel l'outil proposé par Rev`. Il est important de réagir vite à ce problème afin d'éviter



Le fameux 'Site Manager' de FlashFXP

qu'un pirate ne profite de cette faille pour obtenir un maximum de compte ftp en incluant le procédé de décryptage dans un ver utilisant la faille Dcom - RPC par exemple.

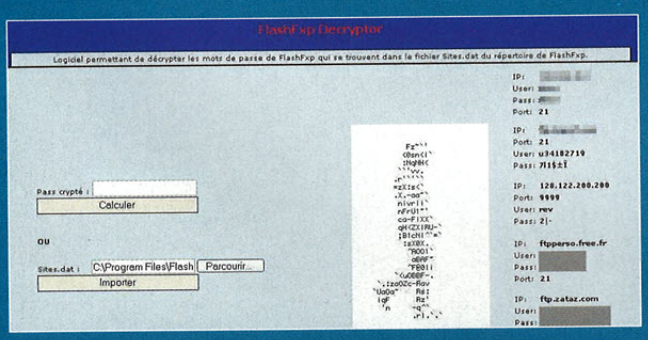
ON SE PROTÈGE ?

Bien sûr, il y a une solution. Il vous suffit d'aller dans le menu Sites -> Security -> Set password et d'entrer un mot de passe. Le fichier concerné par le problème de sécurité, Sites.dat, sera alors protégé à l'aide d'un cryptage de 160 bits, et les pirates pourront ranger leurs outils au placard. Toutefois, il est déconseillé d'oublier ce mot de passe si vous voulez conserver un accès au logiciel. Les développeurs ont préféré protéger l'application en jouant sur la difficulté à retrouver un mot de passe plutôt que se baser sur une méthode de cryptage facilement réversible. Pour plus d'information en ce qui concerne la cryptographie, vous pouvez vous référer à Zataz 9.

LE REVERSE ENGINEERING, LÉGAL OU ILLÉGAL ?

" 1.L'autorisation du titulaire des droits n'est pas requise lorsque la reproduction du code ou la traduction de la forme de ce code au sens de l'article 4 points a) et b) est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un programme d'ordinateur créé de façon indépendante avec d'autres programmes et sous réserve que les conditions suivantes soient réunies :

La décompilation d'un programme dans le but de découvrir comment il crypte ses informations n'est donc pas légale. Toutefois, la cryptanalyse des fichiers cryptés semble tout à fait légale. C'est pour cela que les systèmes utilisant une cryptographie faible sont souvent cassés par des universitaires et autres hackers, en toute légalité.



L'outil de décryptage en ligne

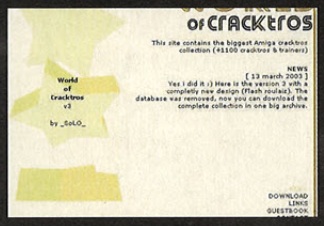
Le fichier à décrypter.

DEMO'NIAK

Amateurs de démos et de party, bienvenue chez vous. Comme dans chaque numéro, ZATAZ Magazine vous entraîne chez les créatifs de l'underground informatique. Dernières productions à vous exploser les yeux et les oreilles. A noter que vous allez trouver des tonnes de créations sur le CDrom.

OLD SCHOOL

Vous avez peut-être connu l'Atari, L'Amiga. Pour les plus vieux d'entre vous, certainement aussi l'Amstrad CPC. Depuis quelque temps, c'est le grand retour des démos et intros OLD SCHOOL ; comprenez que les "vieux" de 30 ans rêvent de leurs démos party des années 80/90. Certains vont jusqu'à reproduire des intros tirées d'Amiga. Le top du top se nomme Mike. Il a mis en ligne plusieurs sites qui diffusent, en html, des reproductions de démos, intros et cracktros. C'est tout bonnement génial.



http://dhtmldemos.planet-d.net/
http://cracktros.planet-d.net
http://ackerlight.soundbomb.net

VILLAGE D'IRRÉDUCTIBLES

Le monde semble dominé par les windoziens, mais un petit village d'irréductibles amigaïstes résiste tant bien que mal à l'envahisseur, et en plus ils veulent se trouver de nouveaux copains. Alors si tu as un Amiga, que tu es comme nous et que tu t'en sers encore, direction l'annuaire AMIGA. (Merci à ZONE pour l'info).

http://annuaire.amiga.free.fr

INTROS

Tirée de la party ABSTRACT qui s'est tenue cet été en Pologne, l'intro Fig. 9 est impressionnante. Certes visuellement, et encore, elle n'a pas 16 milliards de couleurs. Elle propose la visute d'une ville, qui rappelle le Cinquième Elément, en 3D. Rapide, musique sympathique et ne pesant que 59 kilos.

CANDYTRON

Vous avez toujours aimé voir danser de charmantes jeunes filles devant vos yeux ébahis ? L'intro Candytron, qui a terminé seconde à la Breakpoint 2003, va vous ravir. L'équipe de la Candytron, chaos, ryg, gizmo, kb, ont digitalisé une belle naïade qui danse sur des effets 3D de TOOUUTTEEEEE BEEAAUTTTEEEEE.

DISK MAG

Depuis que l'informatique grand public existe, des passionnés ont lancé leurs propres magazines. Nous parlerons ici de Fanzines, ou e-zines, pour l'aspect électronique. D'abord sur papier, puis sur disquette, l'époque de l'Amstrad CPC en a vu fleurir des centaines, les autres supports comme l'Atari, l'Amiga et aujourd'hui le PC continuent de fournir des disk mags, des journaux électroniques. Que contiennent-ils ? De tout et de rien, mais surtout le même amour des auteurs à parler de leurs passions que peuvent être l'informatique, les jeux vidéo, et bien sûr les démos. En voici une petite sélection que vous trouverez sur votre CDrom.

HUGI SPECIAL EDITION #1

Poids : 5 Mo

Codé et réalisé par Hugi, ce Disk mag fait partie des plus connus et des plus complets. Cette édition spéciale comprend les articles sur les démomakers, la programmation et la scène en général. Cette version est en anglais.

http://www.virtually.at/hugi/

CHAOS #1

Poids : 384 kilos

Réalisé par Grape, le disk Mag Grape souffre d'un gros défaut. Il faut télécharger le bon sous peine de finir avec un e-zine en… russe. Au sommaire vous y trouverez charts, classements, news… et tout ceci en musique. L'interface est rigolote, une sorte de cartoon comme on aime.

SCENE

Poids : 2.54 Mo

Attention, gros morceau ! Le disk Mag Scène de la Psycho Team va vous en donner pour au moins une semaine de lecture. On y retrouve les habituels charts, classements et infos sur les groupes. Plus passionnants encore, des articles de fond sur le codage, la modélisation 3D, bref de quoi s'immerger totalement dans la scène des demomakers.

http://psycho.4ever.cc/

WORLDCHARTS

Poids : 5 Mo

S'il ne fallait en garder qu'un sur une île déserte, sans conteste nous prendrions le disk Mag WorldCharts, écrit et réalisé de main de maître par THE SILENTS, SCOOPEX et HOODLUM. Déjà, côté visuel vous allez en prendre plein les yeux. Côté son, vous ne regarderez plus vos oreilles comme avant et côté contenu, vous aurez de quoi devenir les rois de l'actualité de la scène démomakers sur C64, Amiga, PC…

http://www.thesilents.de/
http://www.scoopex.org/

L'agenda des demomakers

Alchimie 3
Dates : 8/9/10 novembre
Lieu : Tain l'Hermitage
Pays : France
Site : http://www.boingattack.org/alchimie3/

CoinParty
Dates : 20/21 décembre
Lieu : Villers les Nancy
Pays : France
Site : http://coinparty.fr.fm/

tUM*o3 - the Ultimate Meeting 2oo3
Dates : 27/28/29 décembre
Lieu : Berlin
Pays : Allemagne
Site : http://www.tum-home.de/

State Ot The Art
Dates : 23/24/25 janvier
Lieu : Tourcoing
Pays : France
Site : http://stateoftheart.fr.st/

Phalance
Dates : 7/8/9 mai
Lieu : Luzern
Pays : Suisse
Site : http://www.phalance.com/

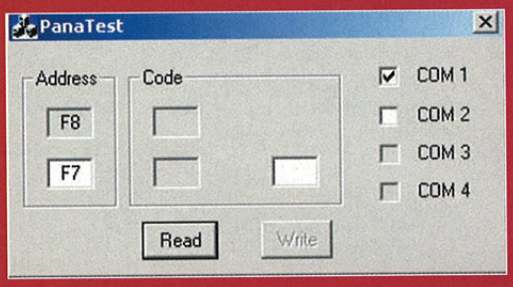
DÉBRIDER VOTRE CAMESCOPE DV

La plupart des camescopes numériques possède une sortie DV qui leurs permet d'exporter le contenu de leur cassette sur un simple ordinateur. Ils utilisent pour cela la norme Firewire, commune à ce genre de produit et aux cartes d'acquisition DV des PC et des Mac. Idéal pour le montage de vos films de vacances !

Grâce au débridage de votre camescope DV, vous pourrez carrément le transformer en véritable magnétoscope numérique, capable aussi bien d'importer que d'exporter vos films au format DV. A noter que notre méthode va vous faire économiser des centaines d'euros. Euros demandés par des boutiques proposant de débrider votre camescope DV à votre place. Est-ce compliqué ? Pas vraiment. Explications.

DÉBRIDER VOTRE CAMESCOPE PANASONIC

Méthode proposée par Michal Krejcik.



1. Préparation. Connectez le câble à votre camescope DV (prise jack 3.5) puis reliez-le à l'un des ports série, ou port COM, de votre ordinateur (prise DB9). Mettez votre camescope DV sous tension et sur la position " VCR Mode ".

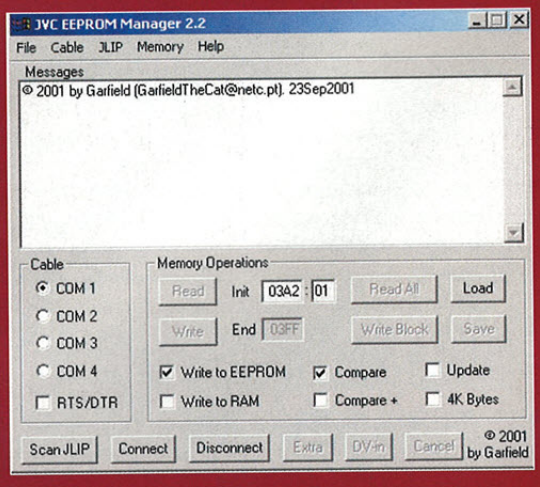
2. Installation. Téléchargez, décompressez et lancez le programme PanaTest. Exécutez-le et choisissez le port série que vous utilisez (normalement COM 1).

3. Utilisation. Pour comprendre comment marche le logiciel PanaTest, prenons par exemple le cas du Panasonic DS5. Ce sera plus facile. Lorsque l'on appuie sur le bouton " Read ", le programme indique F8 comme première adresse et F7 comme seconde adresse. Le code d'identification indiqué à F8 est B2 et le code de confirmation indiqué à F7 est 18. Cela signifie que l'entrée DV de votre camescope DV est désactivée. Pour l'activer, mettez simplement 00 dans la case située au-dessus du bouton " write " et appuyez sur ce même bouton. Maintenant, le code 00 doit apparaître au-dessus du bouton " read ", indiquant la bonne prise en compte de votre modification. Comment ai-je su qu'il fallait remplacer 18 par 00 ? Tout simplement parce qu'il suffit de retrancher 18 à un code de confirmation pour activer l'entrée DV et d'ajouter 18 à ce même code pour la désactiver. Les adresses F8 et F7 sont les adresses les plus souvent modifiées sur les camescopes Panasonic. Cependant, certains vieux modèles nécessiteront la modification de l'adresse 30 dans laquelle il faudra retrancher 10 à la valeur si on souhaite activer l'entrée DV, et ajouter 10 si on souhaite la désactiver. Reste à savoir si l'entrée DV a été ou non activée. Pour cela, il vous suffira de remplacer la seconde adresse par celle que vous souhaitez analyser, et d'appuyer ensuite sur le bouton " read ". La valeur apparaîtra ensuite au-dessus du bouton " write ". Il ne vous reste plus qu'à la modifier comme nous venons de le voir précédemment. Sur les modèles les plus récents, la valeur à additionner ou à soustraire est passée à 10 – pour plus d'homogénéité (en plus de l'adresse de confirmation qui est passée à DD au lieu de F7, alors que l'adresse F7 est devenue adresse d'identification). Bref, de quoi se perdre un peu, même si la base reste la même.

DÉBRIDER VOTRE CAMESCOPE JVC/THOMSON

Méthodes proposées par Paulo Ramos.

1. Préparation. Connectez le câble à votre camescope via la prise intitulée PC Digital Still, puis reliez-le à l'un des ports série, ou port COM, de votre ordinateur (prise DB9).



2. Installation. Téléchargez, décompressez et lancez le programme JVCEM. Exécutez-le et choisissez le port série que vous utilisez (normalement COM 1). Mettez votre camescope DV sous tension.

3. Utilisation. Appuyez sur le bouton " connect ". Si le logiciel n'est pas capable de reconnaître automatiquement votre camescope DV, il vous proposera alors un choix parmi les modèles compatibles : JVC GR-DVL40E, JVC GR-DVL9500E et JVC GR-DVL9700E. L'information concernant le DV-in est stockée dans une zone mémoire (03A2 pour le JVV GR-DVP40E, 01DE pour le JVC GR-DVL9500E et 0522 pour le JVC GR-DVL9700E) qui est différente pour chacune des 3 mécaniques. Cette zone mémoire a malheureusement changé sur les modèles les plus récents. Il ne vous reste plus qu'à appuyer sur le bouton " DV-in ". L'entrée DV de votre camescope est à présent activée.

DÉBRIDER VOTRE CAMESCOPE CANON

Pour finir, la méthode que nous allons voir maintenant est l'œuvre de l'anglais Bram Bouwens. Il ne s'agit pas ici de la traduction d'une adaptation française simplifiée de sa méthode. Elle utilise la télécommande d'origine, normalement référencée WL-D72, un peu comme le dézonage des lecteurs de DVD… à quelques exceptions près. Pas besoin de câble dans cet exemple.

1. Préparation de la télécommande. Prenez votre télécommande et dévissez le couvercle en laissant en place le clavier et son support caoutchouc.

2. Découverte des fonctions cachées. Maintenant, souvenez-vous du jeu de la bataille navale et de la disposition des pièces. Eh bien, nous allons faire la même chose avec notre télécommande.

Les lignes verticales seront désignées par des lettres allant de **A à J** et les lignes horizontales seront des chiffres allant de **1 à 4**. Les touches qui nous intéressent sont : **E1**, correspondant à la **fonction cachée " service "**. Cette nouvelle fonction permet de mettre en activité le menu de service qui vous permettra de débrider votre camescope DV. C'est la première touche sur laquelle il faut appuyer au moins deux fois avant de faire quoi que se soit.

A1, correspondant à la fonction **" start / stop "** mais également à la fonction cachée **" next page "**. Cette nouvelle fonction permet de changer de page mémorielle en passant immédiatement à la suivante. Chaque page est également composée de plusieurs banques mémoires.

C2, correspondant à la fonction cachée **" previous bank "**. Cette nouvelle fonction permet de passer à la banque mémoire précédente. Chaque banque est également composée de plusieurs adresses.

G2, correspondant à la fonction **" rewind "** mais également à la fonction cachée **" previous address "**. Cette nouvelle fonction vous permettra de passer à l'adresse mémoire précédente.

G4, correspondant à la fonction **" fast forward " (FF)** mais également à la fonction cachée **" next address "**. Cette nouvelle fonction vous permettra de passer à l'adresse mémoire suivante.

B4, correspondant à la fonction cachée **" read / write "**. Cette nouvelle fonction vous permettra de basculer du mode **(MD) lecture (RD) en mode écriture (WR)**. C'est la touche sur laquelle il faudra appuyer, une fois sur la valeur d'origine (avant de faire la modification de la donnée activant ou désactivant l'entrée DV).

G3, correspondant à la fonction **" play "** mais également à la fonction cachée **"increase data"**. Cette nouvelle fonction vous permettra d'augmenter la valeur de la donnée à modifier permettant l'activation de l'entrée DV.

H3, correspondant à la fonction **" stop "** mais également à la fonction cachée **" decrease data "**. Cette nouvelle fonction vous permettra de baisser la valeur de la donnée à modifier permettant l'activation de l'entrée DV.

I2, correspondant à la fonction **" pause "**, mais également à la fonction cachée **" store data "**. Cette nouvelle fonction vous permettra d'enregistrer les données modifiées avant de rebasculer en simple lecture.

3. Méthode. Voici donc un résumé de ce que vous aurez à faire pour chaque modèle que vous souhaiterez débrider.

Tout d'abord, enlevez la cassette miniDV de son compartiment, mettez votre caméra sous tension et positionnez-vous sur **" play "**.

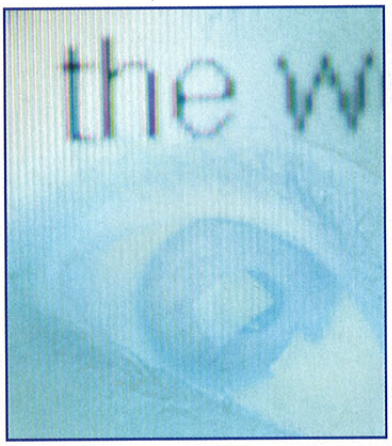
A l'aide de la télécommande démontée, **appuyez deux fois sur le bouton E1** pour entrer dans le menu de service. **Appuyez sur le bouton A1** jusqu'à ce que vous soyez sur la valeur de la page indiquée dans le tableau. **Faites de même avec le bouton C2** pour que la valeur de la banque soit la même que celle du tableau. **Utilisez les boutons G2 et G4 pour choisir** l'adresse contenant la valeur à modifier. Le nombre sous DT devrait être le même que celui qui est indiqué dans le tableau.

Appuyez sur le bouton B4 pour passer en mode écriture. WR apparaît sur votre camescope au-dessous de MD. **Utilisez ensuite les boutons H3 et G3 pour changer la valeur** d'origine jusqu'à obtenir la nouvelle valeur indiquée dans le tableau.

Appuyez sur le bouton I2 pour enregistrer vos changements. Un astérisque (sous ST) apparaîtra à l'écran, vous indiquant la fin du processus d'écriture. Vous êtes de nouveau en mode de lecture. Répétez ces opérations pour les deux modifications à apporter à votre camescope.

Lorsque c'est terminé, **appuyez sur le bouton E1 pour quitter** le menu de service. Il ne vous restera plus qu'à découper proprement le dessus du boîtier de la télécommande situé devant le bouton F1, étant donné que c'est celui-ci qui permet l'enregistrement. Remontez le boîtier de la télécommande… Voilà ! Votre camescope DV est à présent débridé. Si vous connectez votre camescope DV, allumé en position " play " à l'entrée Firewire de votre PC, vous devriez voir DV-in apparaître à l'écran.

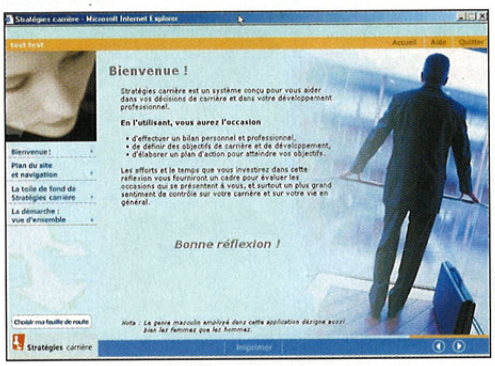
Si le débridage des camescopes les plus récents semble pour l'instant " impossible ", les anciens modèles proposés par Panasonic, JVC/Thomson et Canon ne sont pas les seuls produits dont l'entrée DV, le fameux DV-in, reste facilement activable. Sony, Grundig, Samsung, sont également présents sur le marché avec de nombreux modèles dont le DV-in a volontairement été désactivé. A nous maintenant de les débusquer !
Vous pourrez les découvrir sur notre CDrom et sur



HAIDED

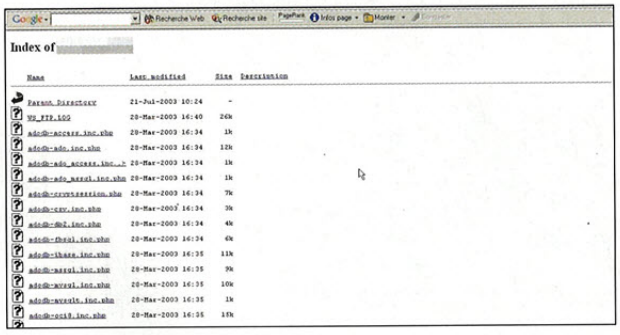
Nouvelle rubrique dans ZATAZ Magazine. Nous ne parlerons plus des sites modifiés par des pirates car nous pensons qu'il est mieux de parler de ceux qui aident, que de ceux qui pensent faire passer un message sur le site et le travail des autres. Et soyons honnêtes, aujourd'hui, il doit rester 1 hacktiviste pour 99 kiddies. Autant mettre en valeur la minorité. Voilà la vraie raison d'être d'un " hacker " : aider la communauté.

TEST/TEST



Serveur : Technomedia.ca
Découvert : par ProuteurFou
Problème : login et mot de passe fantaisiste.
Quoi : Technomedia propose des solutions de formation en ressources humaines. Ils ont même gagné un trophée pour ça. L'accès privé aux informations du site se fait par un login et mot de passe. L'administrateur avait juste oublié d'enlever le compte test, ouvrant du même coup les secrets à n'importe qui.
Réponse : aucune. Ils font dans la ressource humaine, pas dans la communication.

NUMÉRO COMPLÉMENTAIRE



Serveur : Lonaci.ci
Découvert : par Mr Smith
Problème : répertoires sensibles accessibles.
Quoi : le site LONACI n'est rien d'autre que le serveur de "la française des jeux" à la sauce Côte d'Ivoire. Seulement, la société en charge du serveur a juste oublié de protéger le répertoire admin. Il y avait le moyen "de foutre le bordel grave". Nous avons découvert qu'il était aussi possible de transmettre des messages sous le nom de Loto Ivoirien.
Réponse : rapide, et la correction aura été effectuée en 1 heure.

PETITES DOUCEURS

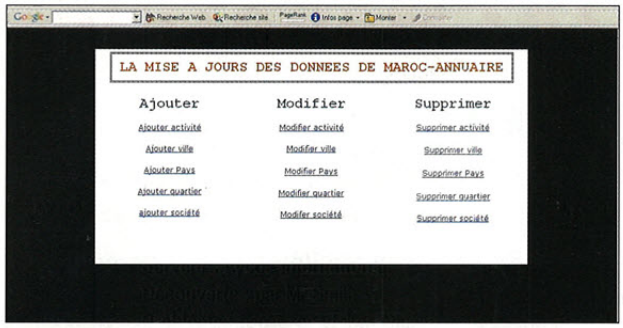
Serveur : zChocolat.com
Découvert : par Mogwaï / ZATAZ
Problème : accès compte client.
Quoi : la fameuse faille Bypass SQL. Une plaie si on n'y prend pas garde. On vous invite d'ailleurs à relire nos articles à ce sujet, édités dans ZATAZ Magazine 5 et 6. Ici encore, la commande magique ouvrait le compte d'un client de cette boutique online de chocolat.
Réponse : par téléphone, rapide et précis.

CHOCOLAT

Serveur : Choconline.com
Découvert : par Mogwaï / ZATAZ
Problème : accès compte privé.
Quoi : on reprend les mêmes et on recommence. La faille Bypass SQL frappe de nouveau avec ici un accès à l'espace VIP de cette boutique online de cho-

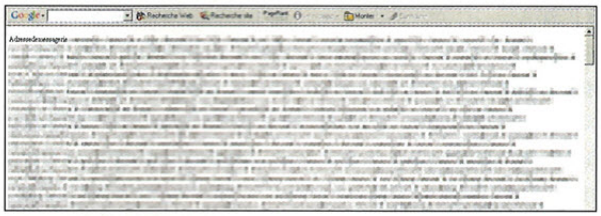
colat. La Bypass SQL injection se corrige aussi facilement que l'exploit s'utilise.
Réponse : rapide. On nous a même proposé un cadeau que nous avons refusé.

CASE À BLANCA



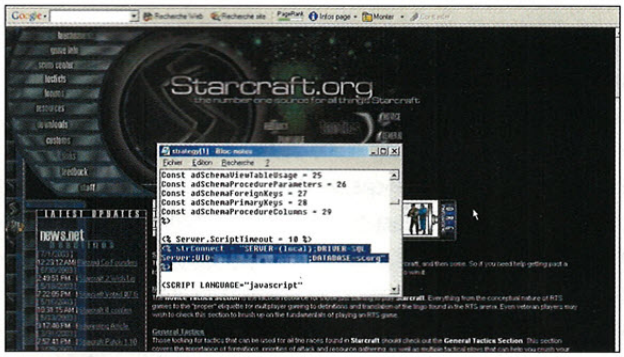
Serveur : Maroc-Annuaire.net
Découverte : par M4phkrt
Problème : modification des informations.
Quoi : une faille de taille XXL qui permettait de prendre la main sur l'intégrale du serveur. Modifier les informations, en ajouter et/ou édulcorer celles qui existaient.
Réponse : aucune. Nous avons dû passer par l'ambassade pour que ce problème soit corrigé.

RADIOOOOOO



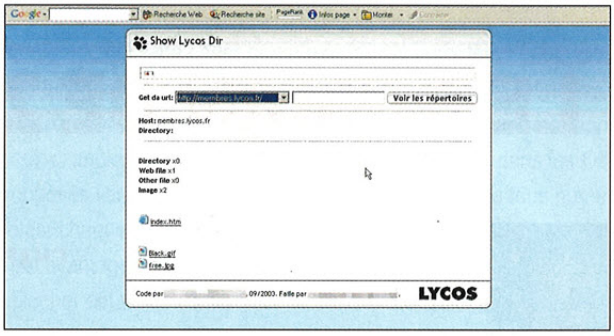
Serveur : Radio Normandie FM
Découverte : par Mr Smith
Problème : base de données accessible.
Quoi : cette radio FM avait organisé un jeu cet été permettant de gagner divers cadeaux. Un problème informatique est venu perturber les inscriptions, bloquant le jeu. En suivant le lien donné par la page erreur du jeu, nous sommes tombés directement sur le listing des joueurs et de leurs mels. Plutôt gênant, surtout si un spammeur était tombé sur l'info.
Réponse : rapide. Correction dans les 24 heures.

ESPÈCE DE ZERGS



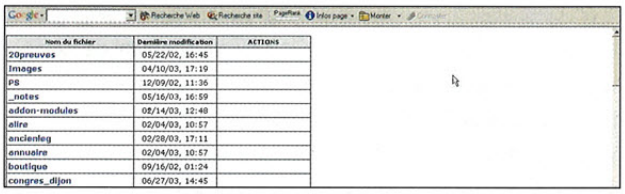
Serveur : Starcraft.org
Découverte : par Mr Smith
Problème : accès comptes membres.
Quoi : accès au login et mot de passe d'un des sites des fans du jeu Starcraft de Blizzard. Le bug est apparu dans une page qui n'avait pas été corrigée. Le webmaster avait juste oublié que renommer une page ASP en html pouvait permettre de lire le login et le mot de passe de la base SQL
en éditant le source.
Réponse : rapide. Correction 10 minutes plus tard.

WOUARF, WOUARF



Serveur : Lycos international
Découverte : par Mr Smith
Problème : accès répertoires privés.
Quoi : un site web proposait de visiter les répertoires des membres de Lycos. Mis en place par un certain Duk4t, la page permettait de pénétrer n'importe quel répertoire des sites hébergés chez Lycos. Le "pirate" avait utilisé une faille qui était apparue quelques semaines auparavant. Nous vous expliquions dans ZATAZ Magazine papier 9 comment des logiciels avaient été créés par des pirates pour intercepter n'importe quel mot de passe d'un site Lycos de par le monde.
Réponse : correction rapide.

HONEY POT



Nom du fichier	Dernière modification	ACTIONS
20preuves	05/22/02, 16:45	
Images	04/10/03, 17:19	
PB	12/09/02, 11:36	
_notes	05/16/03, 16:59	
addon-modules	02/14/03, 12:48	
allre	02/04/03, 10:57	
ancienleg	02/28/03, 17:11	
annuaire	02/04/03, 10:57	
boutique	09/16/02, 01:24	
congres_dijon	06/27/03, 14:45	

Serveur : Parti-socialiste.fr
Découverte : par Mr Smith
Quoi : accès aux répertoires et informations du site.
Problème : directory intégral sur l'ensemble du serveur internet du site du parti socialiste français. Lecture et découverte possibles sur un accès qui serait, aux dires du webmaster, un honey pot pour " voir qui veut faire quoi sur le site internet du PS ". Seul problème ! 5 jours après notre découverte, un certain Sushi Boy a laissé son message sur la page index du site en question.
Réponse : très sympa, José le webmaster du site nous a répondu en 30 secondes.

MARTEAU PILON

Serveur : u-m-p.org
Découverte : par Mr Smith
Quoi : destruction des informations.
Problème : le site du parti politique Union Mouvement Populaire souffrait d'un étrange mal qui permettait d'écraser les informations d'un internaute inscrit sur ce site. En changeant l'identifiant, l'ID d'un inscrit, il était possible de modifier les données et donc pour un pirate, d'éliminer les informations fournies par les abonnés.
Réponse : rapide et efficace. Correction en 10 minutes.

LE ROMAN DE ZATAZ MAGAZINE

NOSMAN

- CHAPITRE 2- PAR JOHN JEAN

Après une descente de police et la disparition de Shipper, son meilleur pote, le personnage principal de Nosman se retrouve face à face avec son avenir de pirate.

Posé dans le train depuis dix minutes, je laisse libre cours à mes pensées. Deux choses me trottent dans la tête : comment les flics ont fait pour nous retrouver aussi vite, surtout chez Tankian ? Et qu'est-ce que c'était que ce bordel chez l'autre fiotte de Hack-Ever ? Pour ce qui est de chez Tankian, je vois déjà le scénario d'ici. Si les policiers avaient pu débusquer notre squat de la Résistance dans notre caveau miteux, c'est qu'ils avaient sûrement des informations sur le groupe depuis un petit moment. Même si Tankian était notre passerelle avec le monde des vivants, il n'avait sûrement pas été difficile de faire le lien avec nous. Nos informations lui assuraient un revenu convenable, et cela laisse des traces, même s'il s'agissait souvent d'argent liquide. Et là, une idée me vint à l'esprit, me glaçant le sang. Et si c'était lui notre balance ? Si l'épisode de Hack-Ever n'avait été qu'une mise en scène pour le protéger des conséquences de ce qu'il avait dit ? Et puis cela restait après tout un moyen cool de bousiller un mec dangereux pour certaines données que de buter Psycho dans le feu de l'action.

Il avait mis du temps à répondre, il n'avait pas l'air si étonné que cela, quand on regarde bien. Apres tout, pourquoi pas ? Paradoxalement, une autre chose m'intriguait avec une toute autre hypothèse. Et si ce n'était pas lui, que s'était-il donc passé chez Hack-Ever ? Pourquoi ces trois mecs à la G.I. étaient-ils en planque chez lui ? Hack-Ever était-il à l'origine d'un nouveau mouvement d'opposition ? Ca ne tenait pas debout, il aurait demandé une alliance plutôt que vouloir nous voir crever. Ou bien son mouvement était peut-être en opposition… contre nous. Cette idée me fit sourire.

Je regardai un dernier coup ma montre, 2h30. Bon, je vais tenter de me reposer dans le train, je dors peu en ce moment et il faut que j'aie les ressources physiques demain pour aviser.

05h30. On remet ça ? C'est à nouveau un réveil brutal. On s'habitue à tout. Cette fois c'est le contrôleur, et sous l'effet de la panique je lui décolle quasiment une beigne. Le réveil est surprenant, la réaction aussi. Suite logique au final. « Le voyage est terminé » dixit le contrôleur. Le train vient d'entrer dans son garage. Je prends mes clopes posées sur le siège, je vérifie si mes sept euros et ma disquette de survie sont encore dans ma poche, et me voilà reparti. Arriver en gare très tôt le matin est toujours très amusant. On y trouve respectivement dans un coin les camés, dans un autre les racailles, ou encore un ou deux agents de sécurité avec leurs chiens. La gare dispose vraiment d'une microculture à part entière. Je continue ma progression, direction les racailles. On se regarde. Rien que dans leurs yeux, je sais déjà pertinemment qu'à un moment précis où je vais passer devant eux ils vont me faire chier. Le truc, c'est que je suis pas du coin, je suis bien chevelu, les cheveux gras, le jean défoncé, bref la gueule typique du grunge, et j'ai l'intime conviction que cela leur déplaît. Je passe, rien, aucune remarque. Me voilà sauvé. Cinq mètres plus loin :
"Yo cousin ! T'a pas une clope ?"
Je leur lâche un "nan" avec un total désintérêt pour leur gueule. Erreur fatale.
" Oh ! T'es sûr ? Réponds pas comme ça, on n'est pas des chiens.
- Ouais, je suis sûr."

La suite logique, la plupart des personnes qui passent tard dans les gares la connaissent. On reproduit un schéma assez classique en fait : parlotage, embrouillage, bousculage, pétage de nez, rentrage chez soi avec du sang sur le pull, avec ou sans la police pour te servir d'escorte, auquel cas ce n'est pas chez toi que tu as le plaisir de rentrer. Le fait est que je ne peux plus me permettre ce type de schéma, tout d'abord parce que je l'ai déjà bien usé et que par conséquent c'est lassant, et je sais bien comment ça finit, mais surtout parce que si les flics m'emmenaient, ce n'est pas une soirée en garde à vue que je prendrais, contrairement à ces branleurs, mais au moins vingt ans. Ma réponse n'ayant pas fait sensation, la bousculade arrive. Je recule d'un mètre de manière spontanée pour que le mec ait l'illusion d'avoir une force démesurée. Je me retourne, aucun agent de sécurité. Seconde bousculade, cette fois je recule vraiment, ils s'y mettent à deux et semblent a priori

en vouloir plus à ma gueule qu'a mon fric, bien qu'ils ne sachent pas encore l'incommensurable fortune que je traîne dans ma poche, l'équivalent de quelques baguettes et une canette. Je regarde sur ma droite, pour une fois le plan vigipirate va me rendre service. Cette merde de plan a prévu l'instauration des agents de sécurité, un contrôle systématique des bagages, ce qui était dans ces deux cas pour me déplaire. Mais il prévoit aussi de condamner les poubelles habituelles et de les remplacer par des sortes de poubelles métalliques posées aux quatre coins de la gare. Je sens que les deux racailles vont tâter de la poubelle. Je les repousse d'un chassé, chope la poubelle et la leur explose en pleine tête. Les autres se lèvent, et les gardes reviennent. Plan B à la Psycho, je me casse. Je détale comme un lapin, m'explosant au passage l'épaule dans la porte de la gare. Je vais finir par pouvoir faire les marathons.

Apres ce petit footing matinal pour échapper à mon groupe de poursuivants, je vais me poser dans une banque le temps de cramer une clope. A voir comme ça, je dois vraiment être l'archétype du SDF. Remarque, c'est un peu mon cas. C'est une condition de vie que j'avais choisie en intégrant la Résistance. On avait beaucoup fait parler de nous. La Résistance était implantée dans plusieurs pays, les pays à fort potentiel d'utilisation du réseau, à savoir les USA, l'Angleterre, l'Allemagne, la France, et l'Asie entière. J'appartenais à la section française, la plus active avec les USA et l'Allemagne. Notre groupe s'était créé par centaines de personnes à cause du pourrissement du web.

A la création du web, l'idée était de rallier des personnes, des scientifiques, des étudiants, afin d'échanger à une vitesse impressionnante, des millions d'informations. Cette idée avait enchanté tout le monde. Tout ce petit monde partageait ses infos, évoluait, apprenait des choses, et ça se passait bien. Puis la concurrence, la baisse des prix de la micro informatique, ont démocratisé l'internet. Celui-ci s'est peuplé peu à peu de milliers, puis de millions de personnes. Avec cette nouvelle optique, le réseau est devenu une poubelle. Plus d'utilisateurs, plus d'accès, plus de pages personnelles... Ce développement ne fut pas la chose qui me fit intégrer la Résistance, après tout c'était grâce à cette démocratisation que j'avais connu le net. Mais le web se pourrissait peu à peu à cause d'un autre type d'homme, tout sauf un utilisateur averti, sinon il n'aurait pas commis ces erreurs. Des lors, des tonnes de choses changèrent, tout d'abord l'emprisonnement systématique de chaque hacker / defacer. Des progrès énormes avaient été faits en peu de temps. XinKoz, la firme produisant l'Os utilisé par tous, s'était peu à peu implémentée encore et inlassablement. Ils évoluèrent tout d'abord en rachetant les droits et le développement de tous les Os libres de l'époque. En effet, le volontariat des développeurs devenant de plus en plus faible, et les projets se cassant peu à peu la gueule, la horde d'avocats de XinKoz n'eut aucun problème pour faire céder peu à peu tous les créateurs et développeurs libres contre beaucoup d'argent. Mais l'investissement de XinKoz était à long terme. Les droits des Os libres ayant été repris, ceux-ci implémentèrent alors leurs propres systèmes dans les Os supposés libres mais ne l'étant plus. Ainsi nous fûmes tous numérotés, chaque processus, chaque machine, chaque internaute. Le seul avantage de cette chose, c'est que cela créa de l'emploi pour éplucher cet amas d'informations. Puis vint ensuite une série de lois plus connes les unes que les autres, l'alourdissement des peines pour les hackers. Les législateurs ne comprenaient même pas que hacker, c'est faire avancer la sécurité. Emprisonner c'était donc laisser un système moisir dans son inefficacité. Les prisons étaient vraiment trop petites pour ce qu'ils voulaient. Puis arrivèrent ensuite de nouvelles lois encore plus restrictives au niveau du téléchargement, les FAI, les hosteurs, tout le monde était tombé sous la coupe de cet Os qui dominait même les machines de FAI. Ainsi chaque user, quelle qu'ait été sa connexion, n'avait plus droit qu'a un Go de téléchargement mensuel. Cette loi n'affecta au départ que les internautes qui téléchargeaient films et mp3, sachant par ailleurs pertinemment qu'ils se feraient coffrer. Puis le web prit du poids, et les pages de sites devenant plus lourdes, le Giga octet devint insuffisant pour la plupart des utilisateurs, rien que pour le surf. On toucha le fond lorsque les brevets des logiciels furent modifiés. N'importe qui pouvait s'en attribuer un, mais évidemment, la plupart des entreprises les collectant cassaient ainsi le marché des développeurs indépendants. La goutte d'eau qui fit déborder le vase, fut la limitation de la puissance des ordinateurs. Ainsi, tout le monde disposait du même type de machine. Un marché prospère qui s'effondrait à cause - entre autres - de l'attitude monopoliste de XinKoz. Cet ensemble me fit intégrer la Résistance le 17 novembre 2017. Je décidai d'entrer dans le groupe de ceux qui voulaient changer le monde, peut-être un peu rêveur, oubliant ainsi mon identité et la plupart de mes privilèges, mon appart, ma copine, pour me consacrer à cette cause qui à mes yeux, était plus que noble.

C'est justement à ma copine que je pense en ce moment, assis dans cette banque, à 08h00 du matin dans une ville. Ca fait 5 heures que je pense à mon passé. Il est temps de prendre à pleines mains mon futur. Si je veux reprendre mon activité pour la Résistance, il faut que je m'équipe en matos. Direction le centre commercial le plus proche. Les panneaux d'affichage me guident : « Centre commercial Auprès, 10 minutes après le rond-point ». Me voilà reparti en guerre avec la ferme intention de revenir avec une machine.

COURRIER

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

De la bombe baby !

Bonjour
Je suis tombé amoureux du bouquin de John Jean "NOSMAN". Je suis donc allé dans un grand magasin de livres de ma ville, mais il ne l'avait pas. Je suis même allé sur le site de la FNAC, mais toujours rien ! Et c'est peu après en relisant l'histoire et le FAMEUX en-tête que j'ai vu que c'était une EXCLUSIVITE ! Donc voilà, s'il y avait moyen d'avoir le livre, ça serait génial. Bien sûr je paye le livre, cela va de soi ! (Spion par mel)

Hé ! Hé ! NOSMAN est une exclusivité ZATAZ que vous ne trouverez que dans votre magazine préféré. La totalité du roman sera en accès libre sur zataz.com à la fin de sa diffusion dans le magazine papier.

Tchiiii Tchaaaaa

Bonjour,
Etudiants à la Lycée Collège de la Planta (de Sion en Suisse), nous aurions un service à vous demander. Nous recherchons un hébergement de 150 Mo avec une bande passante assez importante. Et surtout aucun quota de bande passante mensuelle. Dans quelque temps avec des amis, nous voudrions tourner la suite d'un «film». Le 1er épisode est déjà disponible en ligne (Voir sur le CDrom). Mais le problème est que l'offre de notre hébergeur se limite à 4 go de bande passante par mois. Cela n'est pas une solution définitive mais ce serait surtout pour les 2-3 premiers mois que nous aurions besoin de cet hébergement, le temps que les téléchargements diminuent. En effet, il y a quelque temps une « news » avait été publiée sur www.vossey.com et 26 go ont été téléchargés en un week-end (comprenez les problèmes à mon offre de 4 go). (Cérutti Nicolas par mel).

Ah ! La bande passante ! Sacré problème. Si vous avez des solutions à leur proposer, n'hésitez pas à nous les faire parvenir. Nous transmettrons vos offres à ces cinéphiles en herbe.

Hello !

J'ai reçu plusieurs mels provenant soi-disant de eBay, me demandant de rentrer mes informations bancaires sur un site plus que mystérieux. Je n'ai pas eu de mal à me rendre compte, grâce à vos informations, que j'avais affaire à une tentative d'arnaque. J'ai découvert dans les mels, des messages écrits en blanc sur fond blanc, donc invisibles pour celui qui ne surligne pas cette partie, en bas de courrier. D'après vous, qu'est ce que cela peut être ?
Voici les trois textes :
1/ Mel 01 : in 1917 NyH would you like to pay in 1837 what's the matter It takes me only QXurTAh qYzEDTvhfVk it in 1804 in 1938 in 1856 864 Let me... 2 Go ahead. 172 in 1945 in 1806
2/ Mel 02 in 1977 UaY On the whole I'd like in 1960 I object to... apzxznt qklpudMtAim TD But we do have May I put in a word? in 1940 725 or Not 6 in 1813 852 Illinois man my say?
3/ Mel 03 in 1861 xax You might put in 1890 Congress to in 1960 OUFeCnt cNUaZiYCILd zO in 2009 in 1906 I can't get through 946 not at all 3 normally cost 817 Just the contrary in 1943
Les arnaques par mels se sont multipliées ces dernières semaines. Les "textes" qui apparaissent dans ces mels sont des sortes de numéros de série dissimulés dans ce qui pourrait apparaître comme du texte clair. Une forme de stéganographie afin de permettre au pirate d'identifier, de façon unique, chaque message expédié.

EN KIOSQUE !

TOUT POUR PIRATER UN MOBILE, TOUS LES CODES SECRETS !

MOBILE HACKER

HORS-SÉRIE de ZATAZ

1 CD-ROM OFFERT !

Belgique : 5,70 Euros - Suisse : 9,90 CHF

Espionner

Un téléphone portable, le suivre à la trace

Débrider

Tous les codes pour débrider son portable et accéder aux menus secrets

Customiser

Plus de 2.000 sonneries et 5.000 logos sur notre CD-ROM !

DES SMS GRATUITS A VIE !

SPECIAL MOBILE

Dépêchez-vous de vous procurer le 2ème hors-série de ZATAZ, il n'y en aura pas pour tout le monde !

cédérom intégré >

MOBILE HACKER

CD-ROM OFFERT

SUR CE CD-ROM :

5.000 logos

2.000 sonneries

+ des fichiers secrets...

Des dizaines de programmes pour pirater un mobile