HACKER news Magazine

Numéro 4 / Septembre-Octobre-Novembre 2001 / Trimestriel

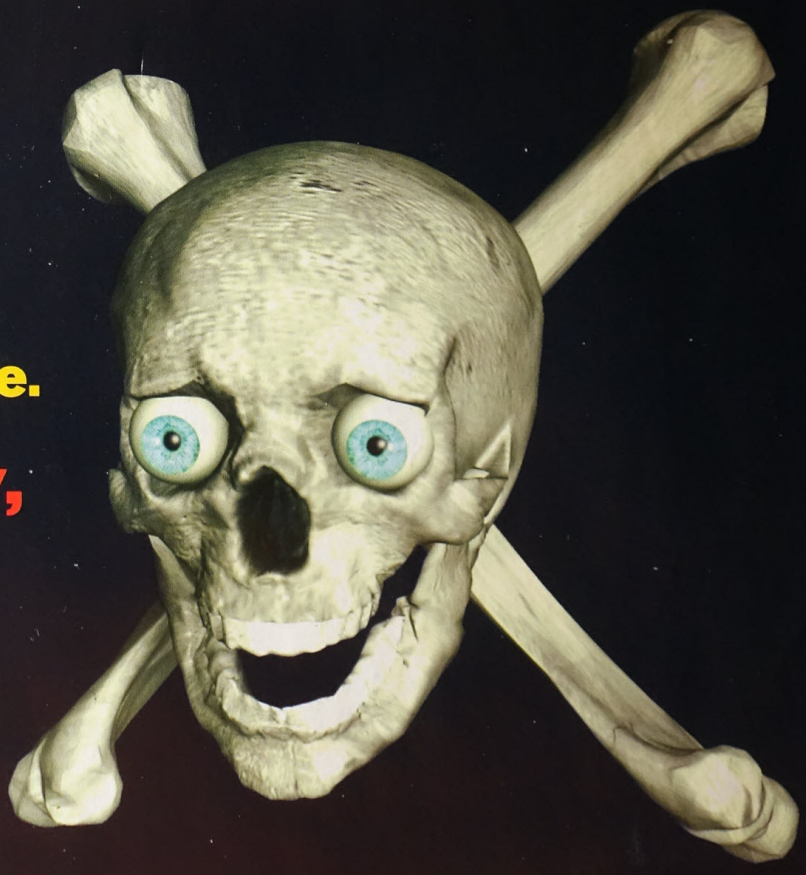
12F

>Téléphone, email, fax,
Souriez, vous êtes fliqués !

>Attaques magnétiques
Comment on peut détruire votre ordinateur à distance.

>Piratage LoftStory,
je t'aime moi non plus !

Tout sur...
Cryptographie, Warez, Espionnage, Intrusion, Mots de passe, Sécurité, Piratage, Carte bancaire...



>espionnage
La panoplie du parfait 007

www.hackermag.com

M 5528 - 4 H - 12,00 F - 1,83 € - RD

Trimestriel - 12 FF - DOM 15F - 85 FB - 3.5 FS - 84 FL - 20 DH - 1400 CFA - $2.95

EDITORIAL

Édito

Vous l'attendiez depuis longtemps, vous en trépignez d'impatience tous les jours chez le libraire du coin ? Eh bien soyez soulagé, il est enfin là, tout chaud sorti de chez l'imprimeur rien que pour vous. Une fois de plus vous allez pouvoir constater que Hacker News Magazine se perfectionne. Plus précis, plus pointu, plus joli aussi et plus clair. Tout ça parce que nous savons qu'on peut avoir l'esprit "Underground" et aimer la perfection. Petite spécificité pour ce numéro, notre ami Philippe vous réserve une pleine page sur les événements de New York vu avec notre regard impertinent mais humoristique... Par ailleurs, Léa, notre héroïne et égérie, est encore en vacances, elle ne nous reviendra que pour le prochain numéro !

Vous avez envie que les choses changent ? Que l'information ne soit pas systématiquement remâchée, prédigérée ? Alors vous allez être content car vous risquez d'en prendre plein les yeux avec votre Hacker News Magazine n°4 !

Eric Le Fauconnier

Hacker News Magazine
150, route de Dieppe
76250 Déville lès Rouen
France
http://www.hackermag.com

Directeur de la publication & Rédacteur en chef :
Grégory Peron

Mise en page : Gouloukri Inzepio, Ozcar Lombrik

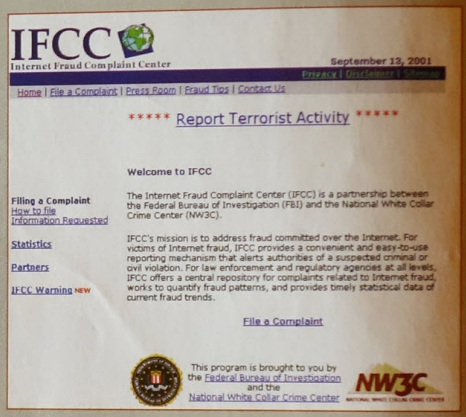
Ont collaboré :
Damien Bancal, DJ GranZ, Kooz, Philippe Tastet, Elvine

Imprimerie: Imprimerie de Compiègne
Commission paritaire : en cours
Dépôt légal : à parution
RCS PARIS B421097973
sarl au capital de 85 000 F

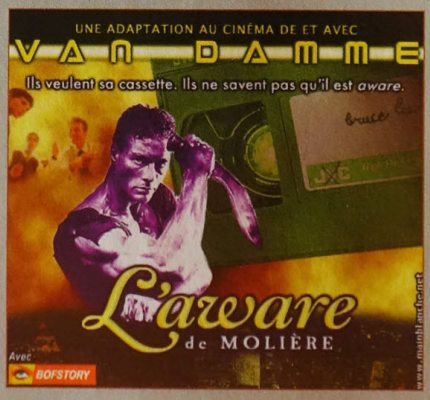
Hacker News magazine est une publication du **Groupe Hagal Aria**

Spécial FAYOTAGE

Le gouvernement américain presse quiconque aurait des renseignements sur les récents attentats qui ont touché New-York et Washington, à venir témoigner. Le FBI a même mis en place un site Web pour que ceux qui le souhaitent puissent rapporter toutes les données possibles et imaginables. Sur le site **www.ifccfbi.gov**, vous pourrez trouver un formulaire à remplir pour délivrer vos informations.



P'tit clin d'œil à tous les "awares" de la terre !



Piratage bancaire

Un Russe de 25 ans, Andrei Golov, a été extradé vers Paris cet été suite à un mandat d'arrêt international délivré par un juge parisien. Salarié dans un centre d'autorisation bancaire moscovite, il a eu accès à des milliers de numéros de cartes bancaires appartenant à des touristes étrangers en visite à Moscou et leurs codes secrets. Il a ensuite ré-encodé ces informations sur des cartes avec piste magnétique vierge pour faire des retraits dans les distributeurs. Un complice aurait bénéficié des précieuses informations en Suède. Les retraits frauduleux ont été effectués en 98 et 99 dans plusieurs pays dont la France, l'Espagne et la Suède. Le procédé transmission / autorisation sur les distributeurs de billets, les codes secrets à 4 chiffres sont transmis chiffrés du distributeur jusqu'à la banque émettrice de la carte. Pour cela on utilise un système dit de "sauts interbancaires", à chaque nœud du réseau, les informations sont décodées et ré-encodées avec d'autres clés : celles du destinataire (à savoir le nœud suivant). Comme toutes les informations ne sont pas chiffrées du début à la fin de la chaîne, il est possible pour un petit malin, introduit au niveau d'un nœud, d'accéder à toutes les informations en clair : contenu de la piste magnétique (notamment numéro à 16 chiffres, date d'expiration, offset), code secret à quatre chiffres. C'est non seulement possible mais cela a été effectué par ce russe et ce n'est pas fait pour nous rassurer ! www.parodie.com/monetique

Virus Caramailien

Un Logiciel nommé Hackbal.zip, un outil de pirate soit-disant capable de pirater les comptes e-mails des clients de Caramail, que l'on trouve un peu partout sur les sites "underground" liés à Caramail cache en son sein un virus trojan. Ce cheval de Troie écrit un fichier dans le répertoire Windows (Nvarch16.exe) et se place dans la base de registre : HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Nvarch16.exe. Si vous avez eu ce programme entre les mains nous vous invitons à vérifier votre PC de toute urgence ;-))

news, rumeurs, news, exclusif, news, préves

>>> les Actualités

Adieu l'artiste

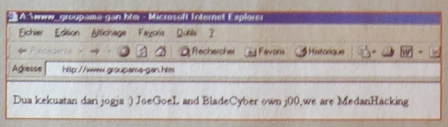
Ingénieur informaticien né en Grèce, Michael Dertouzos vient de disparaître subitement a l'age de 64 ans. Apres des études au Massachusetts Institute of Technology (MIT), il est nommé directeur du Technology Laboratory for Computer Science de cet établissement, un poste clé où sa vision de l'évolution de l'informatique est devenue légendaire. Dès 1974, il annonce que dans vingt ans, un ménage américain sur trois possédera un ordinateur. En outre, il entrevoit déjà le "marché de l'information" qui va exploser avec l'arrivée d'Internet. C'est également Michael Dertouzos qui a empêché l'éclatement de la Toile grâce à la création du WWW Consortium, garant d'un langage unique reliant tous les utilisateurs d'Internet. Il était parmi les critiques les plus féroces de l'orientation prise par l'informatique, peu soucieuse des véritables besoins des utilisateurs. Dans son dernier ouvrage intitulé "The Unfinished Revolution" et à travers son projet "Oxygen", il défendait l'idéal d'une science plus citoyenne.

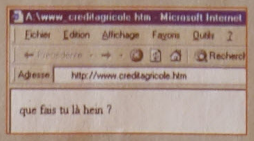
Rencontre autour d'un VIRUS

Le Collectif Artekno entend défendre l'idée d'hybridation. Organiser une rencontre autour du thème du virus répond parfaitement à cet objectif. Tout d'abord, le thème est d'actualité : les contaminations et attaques virales de toutes sortes prolifèrent dans notre société urbaine et fortement technique. Les virus biologiques comme le sida ou la grippe, les virus informatiques comme "I love you" et d'autres encore plus obscurs agressent quotidiennement notre environnement. Tous les artistes qui ont présenté des projets, pour l'opération "VIRUS 2001", ont eu la totale liberté de décliner leurs idées personnelles quand à cette notion de virus. Certains l'ont perçu de manière plutôt littérale, d'autres y ont trouvé le moyen de développer une métaphore autour du monde des médias, d'autres encore l'ont surtout compris sous son aspect envahissant. Pour être efficace, la manifestation elle-même devait ressembler ou se comporter comme un virus. Il faut délocaliser, envahir, répandre le plus possible, d'où l'idée de fonctionner en partenariat avec nombre de lieux dits "intermédiaires", afin de répartir au mieux les travaux sur l'ensemble du territoire parisien. L'opération "VIRUS 2001" est une manifestation regroupant des artistes ou des collectifs artistiques travaillant soit selon des pratiques transversales mêlant danse, son, image et Internet, soit sur une imagerie pratiquant le détournement, l'incrustation et le "parasitisme". Tous les travaux seront présentés dans un ensemble de lieux répartis sur tout le territoire parisien, non pas selon un principe de parcours défini, mais selon un principe de programme aléatoire à choix multiples. Ca doit se dérouler mi-novembre et cela a l'air pas mal, à découvrir donc. www.artekno.com

Defaced

L'été fût très chaud pour les sites Web français. Plus de 200 attaques recensées, 116 en juillet et 106 pour le mois d'août. On retiendra dans cette masse d'attaques, le site du parlementaire Schneinder, par un pirate nommé aCid fAlz ou encore les sites des assureurs axa-assistance par le pirate prénommé tty0 et Groupama-gan par le groupe MedanHacking. On termine avec une banque, celle du Crédit Agricole, dont le site a été modifié par AloneTrio.





4 mois de prison pour un pirate

Raymond Torricecli, alias "Rolex" du groupe de pirates Conflict, vient d'écoper de 4 mois de prison et de 4 000 dollars d'amendes pour avoir piraté les ordinateurs du Jet Propulsion Laboratory (JPL) de la NASA à Pasadena en Californie. Il avait utilisé le serveur pour placer un forum de discussion consacré au piratage. La police a découvert qu'il avait lancé des sites pornos sur lesquels ils utilisaient les numéros de cartes bancaires de ses clients pour rembourser ses communications téléphoniques. Bilan de la seconde fraude, 70 000 francs. Tout n'est pas rose sur le Net ;-)

Cyber menottes ?

Le premier commissariat de cyber-policiers indiens a ouvert ses portes le 15 septembre dernier à Bangalore. Exclusivement chargés de résoudre les crimes de pirates informatiques, tels que les intrusions, les destructions de données ou les fraudes en ligne, l'ancienne cellule d'experts provenant de l'entreprise Infosys Technologies, de l'Institut indien des sciences et de l'éditeur de logiciels Wipro Ltd, basé à Bangalore, a obtenu le statut de commissariat et aura pour juridiction la province du Karnataka, explique un responsable de la police.
www.ccps.karnatakastatepolice.org

Problème bancaire

Plusieurs milliers d'Américains ont eu un retour de vacance difficile avec la découverte de débits bancaires étranges. Pas moins de 3 000 personnes, dans la région de Washington, ont ainsi remarqué que leurs comptes bancaires avaient été ponctionnés de quelques dollars. La First Virginia Banks Inc. et la SunTrust Banks Inc. ont mis sous surveillance certains des comptes de clients afin de savoir d'où peut provenir le "problème".
(Source : www.thestandard.com)

NEWS en bref

news, rumeurs, news, exclusif, news, brèves,

Cyber traque

Singapour et la Belgique viennent de signer un accord qui a pour but de mettre en place des alertes en cas d'attaques virales. Cet accord est destiné à combattre la menace que font peser les virus sur l'économie mondiale. Un type de partenariat dont la France pourrait bien s'inspirer…

Thriller

Bambi, alias Michael Jackson, se demande encore comment deux radios new-yorkaises ont pu diffuser une de ses nouvelles chansons alors que même la maison de disque n'avait pas eu en main le master final. "You Rock My World", le nouveau single du roi de la Pop diffusé a, semble-t-il, été "emprunté" dans les studios. Il suffit ensuite de chercher sur le web pour le trouver déjà en plusieurs milliers d'exemplaires. Ah ! Le marketing viral, belle invention.

Du porte à ports

Pas forcément la news la plus passionnante du moment mais pour info, voici les ports les plus utilisés par les pirates cet été. Une info qui provient du groupe de travail SANS. Alors dans ce top 5, le port 0. Un port "0" qui indique que le port cible est inconnu. Des "ICMP packets" peuvent également s'enregistrer comme un port "0". Le port 53, tcp Domaine, DNS serveur et 53 Udp domaine, DNS Serveur port. Le port 80 : 80 tcp [trojan AckCmd], 80 tcp http, 80 tcp www, 80 udp http et 80 udp www. Le port 137, tcp netbios Name Service. On termine par le port 33 434.
www.incidents.org/cid/query/top_10port_7.php

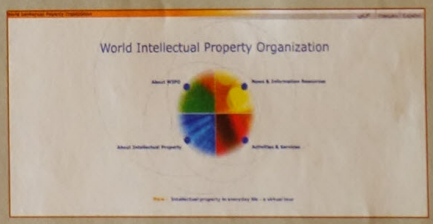
25 ans et moins de dents

Dmitry Sklyarov, arrêté après le rassemblement de hackers de Las Vegas, le defCon, risque pas moins de 25 ans de prison. Ce jeune programmeur russe de 27 ans a eu la mauvaise idée de développer une application qui permet de lire et copier sans restriction les livres électroniques protégés au format PDF. La plainte, déposée puis retirée par Adobe, visait à faire respecter les lois sur les droits d'auteur électronique. Dmitry a été arrêté par le FBI le 16 juillet dans une action prénommé "Travesty". Sous la pression médiatique, Adobe a annulé ses poursuites. Le problème est que la justice US veut faire un exemple, et Dmitry ne peut plus quitter les USA car il a été inculpé par la Cour fédérale de San José. Il doit répondre de cinq chefs d'accusation et risque 25 ans de prison et 500 000 dollars d'amende. Dans la foulée, on apprenait que le format de l'e-book de Microsoft avait connu lui aussi les affres d'un hacker qui aurait découvert une faille rendant la sécurité de Microsoft Reader caduque. Le développeur, anonyme, a fait passer le message par le Massachussetts Institutes of Technology (MIT), et n'a pas l'intention de se faire connaître. Tu m'étonnes !

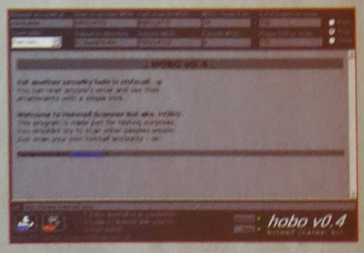
So British !

Deux tiers des entreprises britanniques victimes de cyber crime. Dans un communiqué laconique, l'agence de presse Reuters a indiqué que 65 % des entreprises britanniques ont été victimes de piratage informatique l'année dernière, d'après une étude publiée par la Confederation of British Industry (CBI). Le piratage, les virus et les fraudes à la carte de crédit sont parmi les préjudices les plus couramment subis par les 148 entreprises sondées. Bien que 69% des entreprises interrogées aient jugé la perte financière négligeable, elles craignent que leur réputation soit ternie. L'étude de la CBI révèle que 53% des sociétés se sentent en sécurité pour le commerce inter-entreprise, contre 32% pour le commerce avec les particuliers. "Cette étude montre clairement que les craintes concernant le risque de pertes financières et l'atteinte à la réputation freinent la croissance du commerce en ligne, spécialement pour le B2C, le commerce destiné aux particuliers", a déclaré le directeur général de la confédération, Digby Jones. Il a appelé le gouvernement britannique à mettre en place une agence nationale destinée à lutter contre le cyber crime, à l'instar de l'Internet Fraud Complaint Center, aux Etats-Unis. Désormais, le principal danger pour les entreprises ne vient pas de l'intérieur, mais des pirates extérieurs responsables de 45% des attaques.

L'OMPI veut renforcer la protection des adresses web



L'Organisation mondiale de la propriété intellectuelle (OMPI) recommande l'adoption de nouvelles règles d'enregistrement des noms de domaine internet afin de mieux éviter les litiges dus au "cyber squattage". Il faut dire aussi que l'OMPI a déjà plus de 30 000 litiges résolus et souhaiteraient que les ardeurs des cyber squatteurs se calment avec l'arrivée des nouveaux préfixes tels que .biz ou .info. Une étude réalisée pendant un an a montré qu'une meilleure protection contre les enregistrements réalisés abusivement par des personnes ne possédant aucun droit légitime sur les noms déposés était requise pour les adresses concernant les pays, les lieux géographiques, les groupes ethniques et les substances pharmaceutiques, et non plus seulement pour les personnes ou les entreprises. Pendant ce temps, le site de l'OMPI a vu son domaine quelque peu malmené par un **wiposucks.com** et **wipo.co.uk**, présenté comme le site de l'Organisation mondiale du piratage intellectuel.



Hotmail troué comme du gruyère !

Après plusieurs failles colmatées, Hotmail a encore connu, cet été, une belle frayeur avec une nouvelle faille qui permettait d'accéder aux comptes emails d'un client de ce fournisseur d'email gratuit. Pour utiliser ce piratage, il fallait ouvrir un compte Hotmail, connaître le login Hotmail de la victime choisie et télécharger un logiciel disponible sur le site d'un groupe de hackers nommé Root Core. La manœuvre n'était cependant pas transparente, il fallait en effet, pour consulter les courriers électroniques de la victime, que le pirate utilise le compte Hotmail qu'il avait ouvert. Mais il est tellement simple d'en ouvrir un incognito !

Les hackers dans le dico

Avec la rentrée, c'est la valse des mises à jour des dictionnaires. A noter l'arrivée du mot "Hacker" dans les dictionnaires Larousse et Robert. Les deux volumes vocabulairentesques ont défini "hacker" par : pirate informatique. En gros, ils ont repris la définition du Journal Officiel sans véritablement écouter le public qui utilise ses deux mots dans des situations pourtant bien différentes ! Pour rappel, un hacker agit dans le bien de tous, afin de faire avancer ses propres connaissances et celles des autres ; un pirate, lui, utilise ses connaissances à des fins criminelles.

Données en filigrane

Prolongeant dans le monde virtuel le concept traditionnel du filigrane sur papier, le filigrane numérique doit protéger les données de copies illégales et garantir leur authenticité. Ces filigranes doivent être suffisamment robustes pour tolérer les manipulations de compression ou de conversion et résister aux attaques des hackers. Christian Neubauer, chercheur de l'institut Fraunhofer IIS a Erlangen, même depuis environ quatre ans des recherches sur les filigranes numériques pour les fichiers musicaux. Il a notamment travaille avec le célèbre inventeur du MP3, le professeur Karlheinz Brandenburg. Depuis octobre 2000, le Docteur Jana Dittman dirige à l'institut IPSI de l'ex-centre de recherche GMD un projet de recherche sur les filigranes pour les médias, connu sous le nom de code H204M. La récente fusion de l'ex-centre de recherche en informatique GMD avec la société Fraunhofer a rapproché ces deux projets qui ont fait une apparition commune sur le forum multimédia international IFA 2001 en août dernier à Berlin. (Source : communiqué de presse de la société Fraunhofer)

La "Palm" de la fiabilité

Voici la déclaration qu'ont fait des experts en sécurité : "Les ordinateurs de poche tels que ceux du leader industriel Palm Inc. utilisent un système d'exploitation de plus en plus vulnérable aux attaques et ne doit pas être utilisé pour stocker des informations critiques et/ou confidentielles." Alors les Palm, petits, pratiques mais pas sûrs ? Voir l'article de CNN à ce sujet : http://europe.cnn.com/2001/TECH/ptech/08/16/security.palm.reut/index.html

La fin des mensonges ?

La CIA serait intéressée par des logiciels détecteurs de mensonges. Deux équipes de recherche américaines sont en train de développer le logiciel "ultime" qui serait capable de reconnaître et d'analyser les expressions faciales. Un logiciel qui a fait tendre le porte-monnaie de la CIA qui voit en cet outil, l'arme presque parfaite pour fabriquer un meilleur détecteur de mensonges. Le professeur Terry Sejnowski, qui mène une des équipes de recherche dans le laboratoire de calcul de neurobiologie à l'institut de Salk, en Californie, appelle cette nouvelle technologie faciale "détecteur d'émotion". L'outil, couplé à une caméra, pourrait, parait-il, être capable de détecter des mensonges en distinguant les gradations plus fines dans une réponse émotive - si la personne est vraiment heureuse, triste ou fâchée, par exemple. L'autre équipe est tenue par le professeur Jeffrey Cohn de l'université de Pittsburgh et de l'université de Carnegie Mellon. Le travail de Cohn est basé sur le système de codage connu sous le nom de "système facial de codage d'action (FACS)" développé dans les années 70. Il définit les mouvements de chacun des 44 muscles dans le visage humain, l'information employée par des experts pour étudier des trames des images visuelles et des expressions des personnes "lues".

Direction case zonzon

Un britannique de 24 ans a été arrêté pour avoir mis son p'tit ver, nommé Leaves, un vulgaire trojan, sur la toile. Le FBI lui a mis la main dessus le 15 juillet dernier. Les gars du FBI traquent le ou les auteurs de Code Red et donc, du coup, il faut s'attendre à une foule d'arrestations dans le milieu des codeurs de virus. A bon entendeur…

Retour de la spirale

La société Symantec a découvert une nouvelle variante du virus Magistr. Il arrive toujours par courrier électronique et tente toujours de vous pourrir la vie en contrôlant votre ordinateur préféré, en l'occurrence… le vôtre ! Pour ne pas être embêté, rien de bien nouveau mais il vaut mieux le redire, ne cliquez pas sur des fichiers joints inconnus.

Code Red dans la pomme

Le virus Code Red, qui aura mis une sacré pagaille dans les serveurs cet été, a donc infecté les versions de IIS fonctionnant sous windows 2000 et NT. Mais ce ver a aussi touché les utilisateurs de Mac (9.x et antérieur) car les multiples connexions au port 80, avec lequel s'amuse Code Red, peuvent faire baisser les performances de Macintosh Personal Web Sharing. Pas mal d'utilisateurs Mac sur le réseau ont ainsi pu remarquer des baisses de performances de celui-ci.

Fraudes à la carte bancaire : même pas peur !

Les craintes d'une explosion des fraudes à la carte bancaire seraient largement exagérées ; c'est du moins ce qu'affirme l'étude de la société britannique Datamonitor communiquée jeudi en exclusivité à Reuters. Les fraudes à la carte bancaire ont connu des sommets en Grande-Bretagne, où le nombre de plaintes a doublé en 2000 (+100%) contre une augmentation moyenne de l'ordre de 65% en Europe occidentale. Dans les cinq plus grands pays européens (Allemagne, France, Grande-Bretagne, Italie et Espagne), la délinquance liée aux cartes piratées représentait 759,2 millions d'euros en 2000, dont 468,89 millions pour le seul Royaume-Uni. Le taux de fraudes reste toutefois modeste, bien qu'il soit difficile de mesurer le nombre de paiements illégaux effectués sur internet, estime l'étude. Elle évalue ce taux à 0,06% en Europe, soit moins d'une transaction sur 1500. Pendant ce temps, le logiciel GeZeroLee n'est plus vraiment discret tant il apparaît partout sur le Web. La rumeur fait état d'une version 2, non distribuée. Les divers forums dédiés à ce logiciel et à la Yescard font aussi état que le créateur de GeZeRoLee, Ge0li, serait en pour-parler avec le GIE et serait aussi en train de déposer un brevet permettant de contrer les Yescards. Des rumeurs difficiles à vérifier, Ge0li n'ayant donné aucune réponse à nos questions. On continue d'enquêter et on vous tient au courant !

Faites vos jeux !

Le Web et la course à la sécurité informatique est propice à toute sorte de surenchère. On a cru assister dernièrement à une pub pour une émission de télé shopping du type " Comment perdre du poids en 5 minutes chrono. " En effet l'une des spécificités du ver Code Rouge résidait dans sa faculté à se reproduire rapidement et à infecter un maximum de serveurs en un minimum de temps. Aussi un chercheur de l'université de Berkeley (USA) a-t-il publié une étude affirmant qu'il était possible d'infecter tous les serveurs vulnérables du Net en 15 minutes. Dans la foulée, des consultants de Silicon-Defense ont annoncé la possibilité de faire la même chose en 30 secondes. Qui dit mieux ? Tout est bon pour se faire de la pub sur internet ces temps ci…
Liens vers les articles : 15 mn : www.cs.berkeley.edu/~nweaver/warhol.html - 30 s : www.silicondefense.com/flash

Oh ! Encore un virus...

A chaque jour son nouveau virus. Voici venir "readme", un ver en Visual Basic qui arrive dans un fichier de 24 kilos nommé Readme.exe. Evitez de cliquer sur ce dernier, comme ont pu le faire plusieurs milliers d'européens. Si jamais vous avez été tenté par ce petit bout de code, voici ce qu'il faut faire pour le supprimer, sinon, il va se propager sous votre nom chez vos correspondants. Pour l'effacer, allez dans votre base de registre et effacez "key" : **HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Run** et en **"value" : macrosoft = "C:\Windows\readme.exe"**. Ce virus arrive, comme d'habitude, par courrier électronique avec comme sujet : "As per your request!" et avec comme texte : "Please find attached file for your review. I look forward to hear from you again very soon. Thank you."

Windows XP décortiqué

Des chercheurs allemands ont mis à jour la nouvelle sécurité de Windows XP. Le plus délirant est qu'il s'avère que Microsoft a tellement bien bossé pour protéger son système qu'il va être plus simple pour les utilisateurs d'utiliser la version "warez" (pirate). Les informaticiens de Licenturion expliquent donc de A à Z comment fonctionne le système de protection de Windows XP et son processus d'activation.
www.licenturion.com/xp/fully-licensed-wpa.txt

Le projet CPCNG

Le projet international CPCNG (48 membres) a pour but la création d'un libre (open source) descendant du mythique Amstrad CPC. Basée sur un eZ80 fonctionnant à un peu moins de 50 MHz, la machine sera dotée de processeurs Risc pour la gestion graphique et sonore. Par exemple le chip sonore traitera en hardware les formats sonores existants, émulera le SID et le AY... Pour le graphisme, tous les formats comme le PNG, le BMP, le JPG seront traités en hardware, il y aura aussi des fonctions 2D et 3D, la possibilité d'avoir 256 sprites hard de taille redéfinissable, de multiples modes vidéo en 24 ou 32 bits (voir même un mode matriciel comme sur la GBA) (on parle de 64 Mo de Ram vidéo au minimum). La machine pourra avoir jusqu'à 1 Go de Ram. Elle disposera de connecteurs IDE, USB, série, clavier (de type PC) ainsi qu'un emplacement pour modem. 1 Mo de Ram sauvegardée par pile sera aussi disponible. L'OS sera en partie en Rom et proposera une architecture multitâche préemptif multithread temps réel, une interface graphique 100% personnalisable. La machine est

repository of free, open source IP cores — OPENCORES.ORG

destinée aux passionnés, aux entreprises car elle pourra faire office de webserver (avec dans ce cas une version spéciale de Linux) et à la famille (en tant que WebTV). L'équipe fait tout pour la produire à moins de 1500 F. L'équipe a d'ailleurs l'honneur d'accueillir un nouveau membre dernièrement en la personne de Roland Perry, l'ingénieur qui avait créé la gamme chez Amstrad, ce qui ne fait que renforcer les possibilités de la machine et l'enthousiasme qui règne autour ! L'équipe recherche encore des contacts alors si vous avez des idées originales, des connaissances en électronique, fpga, vhdl etc., n'hésitez pas à les rejoindre sur **www.egroups.com/group/cpcng**. Le site web est **http://cpcng.free.fr/index.htm**. Reste à espérer que le projet ira jusqu'à son terme... Pour en savoir un peu plus, retrouvez notre article page 15 !

Quand le copyright étouffe la liberté

L'avenir ne semble pas tout rose Outre-Atlantique. Avec leur manie de tout légiférer et de tout réprimer, les Américains, inventeurs du Net, vont le détruire. Le Sénateur Hollings vient de proposer une loi qui fait froid dans le dos. Baptisé Security Systems Standards and Certification Act, le texte prévoit tout simplement qu'il sera illégal de "manufacturer, importer, offrir au public, fournir ou trafiquer de quelque manière que ce soit un appareil numérique interactif et n'utilisant pas de technologies de sécurités certifiées". En d'autres termes, adieu les MP3, adieu la vidéo en ligne venant de France, etc. Réjouissant non ?

Le FBI pas très clair...

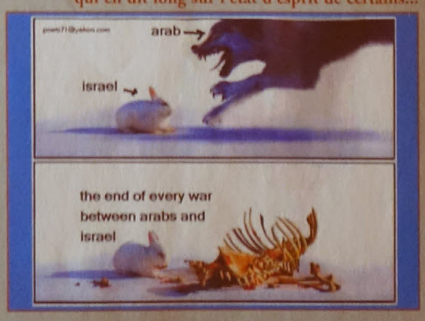
Federal Bureau of Investigation
www.fbi.gov

Le FBI n'a pas fourni d'explications probantes sur la méthode utilisée il y a quelques mois pour pirater le PC du fils de la Mafia et démanteler toute une filière mafieuse. Le Bureau aurait bugué le clavier de Nicodemo Scarfo (on se croirait dans le Parrain !) après qu'il ait échoué dans l'ouverture de fichiers cryptés sur son disque dur. Les avocats de Scarfo ont objecté que ces méthodes n'étaient pas conformes et que, du même coup, les preuves ne pouvaient être prises en compte. Le FBI refuse de donner plus de détails sur la méthode utilisée, invoquant des raisons de sécurité nationale... On croit rêver. Bref, le FBI bafouille, s'accroche aux branches et Scarfo rigole !

Arnaque à la télévision

La société canadienne Visual Labs Inc. tire le signal d'alarme : son tout dernier produit serait totalement bidon. Le responsable de l'entreprise aurait bidonné une démo du prétendu nouvel écran plat maison en présentant un téléviseur acheté dans un magasin d'électronique. Sheldon Zelitt, le fondateur de la société, a été suspendu. Il a donc essayé de faire passer un écran plasma d'une valeur de 11000 dollars (acheté avec l'argent de la société) pour un prototype de Groutfree, la dernière création de Visual Labs. On ne peut pas dire que ça fasse très sérieux :-).

Et pour la bonne bouche, une drôle d'image qui en dit long sur l'état d'esprit de certains...



Les pirates chinois se réveillent

Les hacktivistes chinois font beaucoup parler d'eux. Après avoir attaqués les sites américains en juin dernier, cet été ils se sont "encore" attaqués au Japon. L'histoire d'amour entre ces deux pays ne date pas d'hier. Les hacktivistes chinois aiment fêter à leurs manières certains anniversaires. En février dernier, et pour la seconde année, le japon avait été attaqué par des pirates pro-chinois pour la commémoration du massacre de Nanjing par l'armée japonaise lors de la seconde guerre mondiale. En l'an 2000, pas moins d'une dizaine de sites du gouvernement japonais étaient tombés sous les coups de pirates chinois. En 2001, on en comptait plus d'une cinquantaine. Aujourd'hui, le groupe HUC, Hackers Union China, qui a fait parler pas mal de lui pendant le conflit numérique entre la Chine et les USA, vient d'annoncer qu'il venait d'attaquer des sites japonais par mesure de représailles contre une visite controversée du Premier ministre japonais à un sanctuaire dédié aux victimes de la guerre. Une trentaine de sites du gouvernement japonais ont du fermer suite à des attaques de type Denial Of Service (DOS). Dans la foulée, des activistes coréens se sont coupés un doigt lors de la visite du Premier ministre au sanctuaire Yasukuni à Tokyo, un mémorial à la mémoire des 2,5 millions de victimes japonaises des guerres. Les (h)activistes n'ont pas apprécié les noms d'une dizaine de criminels de guerre parmi les noms notés dans ce sanctuaire. C'est quand même très étrange que des pirates chinois soient aussi actifs dans un pays aussi policé ! D'ici à penser qu'ils pourraient être tolérés par le régime en place, voir soutenus, il n'y a qu'un pas...

Top 5 Virii

Voici les 5 virus les plus présents cet été sur le Web. Un classement réalisé avec les principaux leaders du marché antivirus. A noter le renouveau de haptime utilisé par certains pirates dans leurs défacements. Ils cachent ce virus dans la page et les visiteurs sont infectés. En première position cet été, LoveLetter, suivi de près par FunLove et le fumeux SirCam, suivit en 4e position de Haptime et dernière place Code Red.

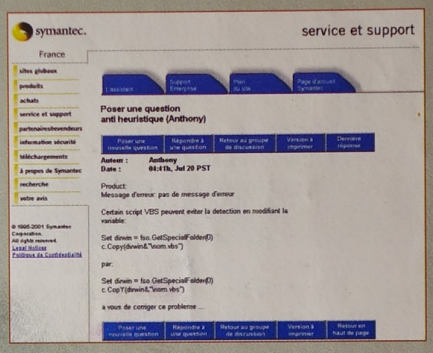
Avez-vous été visité par Code Red ?

Un petit programme permet de savoir combien de fois code red est passé par chez vous. Il se nomme php redcode, c'est le site Danois Zbox (www.zbox.dk/download.php?op=mydown&did=22) qui propose de télécharger ce petit code PHP. Il paraît que certains serveurs ont eu la visite de ce virus plus de 300 fois. Un vrai bonheur...

Caramail, cible des script kiddies français !

Savez-vous quel est le site Web le plus attaqué par les pirates en France ? Non, ce n'est pas Microsoft, mais le fournisseur d'email, forum, chat, Caramail. Ici pas de modification de pages, mais des vols de mots de passe, des détournements d'emails, des éjections de chatteurs sans aucune forme de raison. En gros, un vrai merdier numérique. Dernier fait marquant en date, des informations appartenant à des administrateurs ont été diffusées, permettant ainsi d'éjecter tout le monde des chats. Il serait bon de sécuriser un peu tout cela et par la même occasion d'avoir un regard plus attentif sur les chat rooms dont les noms sont parfois très explicites (du genre "j'aime les petits n'enfants tout nus" si vous voyez ce que je veux dire).

Norton ne dit pas merci



Un internaute français, Anthony, a découvert voilà quelques semaines comment tromper Norton AntiVirus. En étudiant le langage VBS, mais aussi la structure des scripts et des virus programmés dans ce langage, il a commencé à trafiquer quelques lignes et a découvert qu'en modifiant la ligne de code

```
Set dirwin = fso.GetSpecialFolder(0) c.Copy(dirwin&"\nom du script.vbs")
```

par :

```
Set dirwin = fso.GetSpecialFolder(0) c.CopY(dirwin&"\nom du script.vbs")
```

cela rendait le script indétectable. Norton ne savait pas faire la différence entre les minuscules et les majuscules on pouvait donc à partir de cette faille écrire des scripts indétectable et relativement dangereux. L'éditeur de Norton, la société Symantec, a été mis au courant de la faille le 20 juillet, une correction est apparue très rapidement... mais le "merci", lui, il se fait toujours attendre !

http://servicenews.symantec.com/cgi-bin/displayArticle.cgi?article=3257&group=symantec.support.fr.custserv.general&next=40&tpre=fr&

Protection caduque ?

Quatre hommes originaires d'Asie ont été arrêtés par le FBI pour contrefaçon de logiciels. Attention, ici la police n'a pas eu à faire à de modestes amateurs de warez, mais un bon gros groupe d'origine chinoise, plus proche d'un groupe mafieux que d'une bande d'ados boutonneux. Lors de la perquisition, les forces de l'ordre ont mis la main sur pas moins de 70 millions de contrefaçons ! Il est intéressant de remarquer que la saisie a mise en évidence l'inefficacité de la toute dernière protection développée par Microsoft, "l'hologramme anti-piratage", qui n'aura décidément pas tenu bien longtemps. Les CD contrefaits en étaient tous équipés. Source : www.inpact-hardware.com/actualites3.php3#id_news_2361

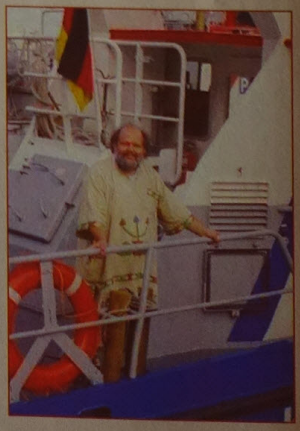
Un bug ravageur

MSN Messager a planté quelques jours début juillet. Perturbé par un problème technique, le système de messagerie MSN a empêché quelques dix millions d'utilisateurs sur les trente millions que compte cette société d'accéder à leurs messageries durant certaines périodes de la journée. Environ 300 000 clients ont perdu notamment l'agenda de leur messagerie et ont du le reconstituer. Microsoft, le concepteur de ce système, pense que le problème ne serait pas lié au système d'exploitation (ben voyons), mais se situerait au niveau des contrôleurs de disque d'un serveur de banques de données fabriqués par Sun Microsystems (l'un des principaux concurrents de Microsoft...). De leur côté, des experts font remarquer que Microsoft utilise des serveurs alimentés par les logiciels de ses concurrents, au lieu de recourir à sa propre technologie Windows, afin d'effectuer certaines opérations très délicates. Il y a un mois, Microsoft avait reconnu utiliser le système d'exploitation à source libre FreeBSD pour ses serveurs Hotmail.

Le CCC en deuil

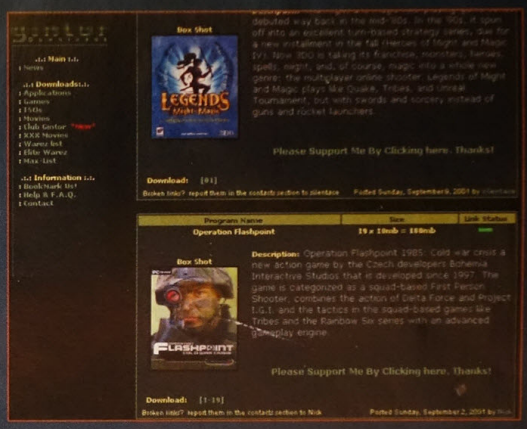
Herwart Holland-Moritz, père fondateur du Chaos Computer Club en 1980, est mort dimanche 29 juillet suite à un problème cardiaque qui l'avait frappé quelques semaines auparavant. Plus connu sous le nom de Wau Holland, il emporte à 49 ans l'une des plus belles pages de l'underground informatique. Le Chaos Computer Club est l'un des groupes de "hackers" les plus respectés au monde qui défraiera la chronique dans les années 80. Un hommage a été rendu à Wau lors du HAL, meeting de hackers, qui s'est tenu au moins d'août dernier. **www.ccc.de**

A découvrir en exclusivité, notre dossier entologique sur le CCC pages 22 & 23



Quinze ans de hacking

Professeur de mathématiques, MaXoR, un pseudo, a écumé tous les systèmes, toutes les machines. Son plaisir ? Casser des protections de logiciels… Pour le plaisir, mais très vite aussi pour l'argent.



Comment as-tu débuté ?

En 1987, j'ai eu comme cadeau par ma famille un ordinateur, un Amstrad CPC. Jeune professeur de mathématiques, j'ai voulu découvrir comment l'ensemble fonctionnait. J'ai très vite pris contact avec des passionnés, on a sympathisé et de fil en aiguille on m'a fourni des jeux à déplomber et c'est ainsi que j'ai débuté.

Tu as déplombé beaucoup de logiciels ?

Sur CPC, je les ai tous crassés. C'est énorme quand j'y repense, mais une fois qu'on y prend goût, on n'arrête plus. A l'époque de l'Amstrad un petit boîtier permettait de déplomber un logiciel très rapidement, le MULTIFACE. Il existait le même boîtier sur Atari et sur la première génération d'Amiga, l'Ultimat Ripper. Aujourd'hui, un désassembleur, un bon cruncheur et le tour est joué.
Je ne parle même pas de ceux qui se contentent du bouton rouge de leur graveur.

Pourquoi préfères-tu le piratage de logiciel ? Pourquoi ne pas avoir fait profiter les entreprises de ton savoir-faire ?

Moi mon job c'est d'être professeur. J'ai eu des centaines de contacts très enrichissants grâce au cracking, des amitiés que je n'aurais jamais eues au sein d'une entreprise, de mon école. On prend un vrai plaisir quand on se retrouve dans des meetings.

Qu'est ce que le WAREZ ?

Warez est un terme générique qui désigne les logiciels piratés. Les Gamez se sont les jeux piratés. Le warez est donc le logiciel réduit pour être utilisable sans protection. Moi je vire les intros qui ne servent à rien, j'arrive même à patcher les bugs d'origine.

Comment est organisé l'univers de la scène cracking ?

Peu de gens touchent les Warez via les BBS, ils vont plus facilement sur des sites web qui proposent soit les cracks, le petit programme qui va permettre la copie, soit carrément la version warez d'un groupe de pirates. En général, les "vrais" sites warez bénéficient de gros débits (écoles, entreprises, administration).

C'est quoi les raisons pour vendre du Warez ?

Arrondir les fins de mois surtout pour les étudiants et chômeurs. Au début c'est pour l'égalité devant l'ordinateur. Cela permet aussi d'essayer les jeux plus en profondeurs avant d'acheter l'original. Les journaux et les sociétés de jeux se foutent de nous avec les versions demies, (les *previews*). Il y a aussi ceux qui veulent une copie de sauvegarde, autorisée par la loi.

Le jeu en vaut-il la chandelle ?

Bien sûr. A 350 francs la compilation, on peut très vite se faire beaucoup d'argent. Moi je tourne aux environs des 20 000 francs (3 000 Euros) par mois d'argent de poche !

RIPPER : Enlever les parties inutiles, qui alourdissent, la taille d'un logiciel. Les vidéos sont exclues des jeux warez.
CRUNCHER : Réduire en taille un logiciel grâce à un algorithme mathématique. On peut réduire un logiciel de 50 % de sa taille dans certains cas.
BBS : Bulletin Board System. Serveur privé joignable par modem uniquement avec un numéro de téléphone précis.

La loi est très stricte avec la copie de logiciel. Il est autorisé une copie de sauvegarde à la condition que vous possédiez l'original. Il est interdit de vendre ou de mettre à disposition cette copie. Les avertissements que vous diffusent les sites de warez, vous précisant que vous pouvez garder une copie 24 heures, sont totalement faux.

NEWS news, rumeurs, news, exclusif, news, brèves,

en bref

Le FBI donne des sous

Un contrat de 3 ans et 2 millions de dollars vient d'être décroché par la société i2 Inc. Contrat avec la version américaine de notre DST nationale, le FBI, afin que i2 Inc réalise un logiciel capable de regrouper des informations lors d'une enquête. Ce logiciel devra être capable de faire le lien entre diverses informations indépendantes. En espérant qu'après Omnivore et Carnivore, d'anciens mais toujours actifs logiciels d'espionnage du FBI, ce nouveau logiciel ne sera pas appelé "Destructor".

La Chine n'aime pas la FM

Les Chinois ne peuvent plus écouter RFI en chinois via le web. Depuis le 13 juillet dernier, soit quelques jours avant la nomination de Pékin pour les JO de 2008, la diffusion via le web des émissions en Mandarin de Radio France Internationale ont été brouillées par les autorités chinoises.

Président vérolé

Les virus facilitent le travail des journalistes en Ukraine. Pour preuve, le virus Sircam a infecté un des ordinateurs de la présidence de ce pays. Le virus se diffusant via la messagerie, il en profite par la même occasion pour copier/voler des documents sur les disques durs infectés. Cette fois le document, reçu par le magazine For-ua, était confidentiel, il donnait l'intégralité des horaires de déplacement du Président de la république Ukrainienne !

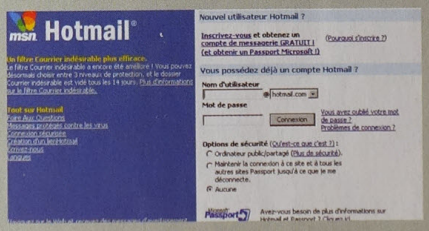
Le Sénégal, c'est chaud !

On pensait à un voyage de mannequins, il s'agissait peut-être de proxénétisme. Les sœurs Campbell et Oumou Sy sont du moins regardées de travers par les autorités qui pensent qu'elles ont participé à un tel réseau. Fin août, une centaine de mannequins sénégalais s'apprête à rejoindre la Libye à l'occasion du 32e anniversaire de la prise de pouvoir par Khadafi. Pourtant l'avion a été bloqué au sol avant le décollage car il semblerait que le vol était destiné à envoyer des sénégalaises vers la Libye pour alimenter les réseaux de prostitution libyens. Une affaire qui jette un froid diplomatique sévère entre la Libye et le Sénégal…

CanalWeb : enfin la fin ?

Il est loin le temps des fastes de Môooosieur le président directeur général, Jacques Rosselin. Après avoir levé plus de 130 MF et les avoir gaspillé en moins de temps qu'il n'en faut, les temps sont durs ! Il faut dire que les locaux spacieux à deux pas de l'Arc de Triomphe où travaillent plus de 130 personnes ça coûte beaucoup d'argent… Ah, mais c'est sur que CanalWeb était l'un des fleurons des startup françaises, un exemple souvent cités par les ''Pros''. Pendant que certains s'inquiètent de leur avenir incertain dans cette société, d'autres n'éprouvent pas ce type de problème avec des salaires confortables (l'attaché de presse du site n'a pas souhaité nous confirmer l'information selon laquelle le salaire du PDG de CanalWeb, Jacques Rosselin, dépasserait les 50 KF). Espérons être rapidement débarrassé de toutes ces reliques qui parasitent la nouvelle économie et qui ne pensent le plus souvent qu'à s'en mettre plein les poches !

Hotmail ou l'email non sécurisé



Et ça continue, la série noire pour Hotmail ! Une nouvelle technique de piratage de ce site vient d'être découverte. En ajoutant un JavaScript dans la ligne expéditeur (From) d'un message envoyé à un utilisateur de Hotmail, un pirate peut éviter les filtres que Microsoft a mis en place pour protéger ses millions d'utilisateurs. Microsoft enquête actuellement et se refuse à tout commentaire. Quoi qu'il en soit, cette technique n'exigerait même pas que le message soit ouvert par l'utilisateur… On doit pas être fier chez Hotmail en ce moment !

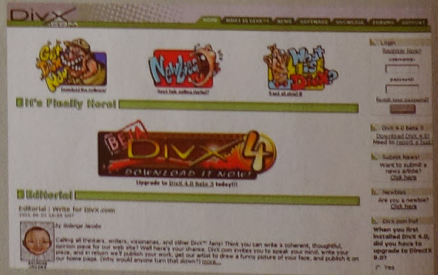
La répression en Chine sur l'Internet s'intensifie

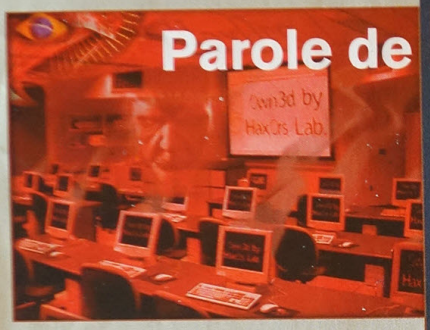
Pas moins de 18 cyber dissidents sont actuellement emprisonnés pour subversion et des centaines de sites ainsi que plus de 8 000 cybercafés ont été fermés au cours des derniers mois pour ces mêmes motifs. L'une des dernières manifestation de la liberté de pensée en date, la fermeture du bulletin Baiyun Huanghe **(bbs.whnet.edu.cn)** de l'Université de Science et de Technologie de Huazong (centre de la Chine), a été ordonnée par le Conseil d'Etat le 5 septembre 2001, à la suite de la diffusion par des étudiants d'articles sur la tuerie de la place Tiananmen. Engagé politiquement, il comptait plus de 30 000 abonnés. Les étudiants pouvaient y échanger librement leurs opinions à propos de sujets interdits par le pouvoir communiste. Toute une série de lois draconiennes sur la circulation de l'information sur Internet ont été adoptées l'année dernière permettant ainsi à une unité de police spécialement créée pour l'occasion, de veiller sur ce qui peut être lu et écrit par les ressortissants Chinois ! Pour en savoir plus : **www.rsf.org** (source : Atelier Weissrock)

DivX 4, DivX news

Une nouvelle version du codec DivX vient de sortir. La version 4.0.3 propose sept grosses nouveautés et corrections de bug. Du tout bon pour ceux qui souhaitent coder leurs vidéos de vacances d'été à LA pour le DefCon ! **http://download.divx.com/videoplayers/theplaya/DivX4FullInstaller.exe**

Quant aux producteurs indépendents, ils viennent de réaliser ce que le DivX pouvait leur apporter, notamment en terme de diffusion sur Internet. Le réseau DivX (DivX Network) est une société qui exploite le codec DivX 4.01, la forme légale du logiciel de compression. Cette société propose actuellement le téléchargement payant d'un film intitulé World and Time Enough ; une comédie de 1995 vendue au téléchargement pour moins de 5$ contre 17,95$ pour la cassette VHS. Les problèmes de diffusion des petits producteurs seraient-ils à conjuguer au passé ? On l'ignore d'autant qu'il apparaît que Warner Bros, Vivendi Universal, Paramount et la MGM ont passé un accord avec le système propriétaire de Sony appelé MovieFly… Plus ça change, plus ce serait pareil ?





Parole de Hacker

A 31 ans, Manu est l'un des plus vieux "hackers" de la scène française et informaticien en Irlande pour une petite entreprise de sécurité informatique. L'underground, ça lui coule dans le sang.

Qu'est que l'Underground ?

Ça dépend des points de vue, le mien étant assez restreint je vois plusieurs définitions. Ça peut être une ou plusieurs des choses suivantes: un monde très fermé et autonome, une énorme source de richesses et d'intoxication culturelle, un état d'esprit à caractère persistant (~= religion ?), une galerie sous terre (catacombes) qui mène à... une soirée techno (sauvage) / un groupe de hackers (sauvages aussi ;-) / une odeur de fumée de chanvre (domestique), une amplitude dans la courbe de température (rien à voir avec le réchauffement de la planète), une organisation improvisée de particules instables dans un chaos artistique total.

Qu'est ce que la scène ?

Représente-toi une scène de théâtre, ses acteurs, décorateurs, le public et les coulisses... Tous ces éléments qui sont rassemblés au nom de l'illusion portent à croire que seuls les spectateurs sont dupés. La scène dont on parle ici est à double face, les spectateurs dont on parle (le public) y sont également des acteurs d'une espèce passive. C'est une passerelle entre l'underground et la surface qui est dressée pour satisfaire la curiosité des gens qui des deux côtés travaillent en coulisses.

N'est-ce pas que du vocabulaire ?

Si le silence est aussi profond que l'éternité, alors la parole est aussi superficielle que le temps qui passe.

Quels sont les groupes, les hackers qui t'ont le plus marqué ?

Sur la communauté francophone (à savoir dans le cyber monde), les groupes qui m'ont le plus marqué sont des groupes comme madchat ou alternative, il y a aussi eu des pionniers comme les 117. Les hackers qui m'ont le plus marqué étaient (et pour certains sont encore) tous les membres de ces groupes ainsi que quelques amis du Québec qui apprécient de rester dans l'ombre.

Pourquoi ?

Pour leur sens de l'éthique et du partage, l'enthousiasme à apprendre et faire apprendre, et leur capacité à faire abstraction de leur ego. Il y a aussi pour certains cette façon de quitter la scène avec un style qui leur est propre.

Le passage de pirate à hacker est-il plus simple que de hacker à pirate ? Y a-t-il une véritable différence ?

Laquelle des deux étiquettes colle le plus dans le dos, personne ne veut savoir... Et les considérations géopolitiques sont trop ambiguës pour admettre une telle nuance lexicale. Les différences ? La marque de la colle, quelquefois le fournisseur.

Comment trouves-tu l'évolution de la scène depuis que tu y navigues ?

Il faut mettre un frein à l'immobilisme !

Comment penses-tu qu'elle va évoluer ?

Elle va probablement évoluer de concert avec les médias qui la bercent, tantôt saut de géant tantôt à pas de loup. Qui peut savoir ? Avec toutes les nouvelles technologies qui émergent et/ou convergent, le wireless, la physique quantique appliquée, les générateurs d'improbabilité et le sabre-laser, peut-être que demain c'est déjà hier...

Que faut-il craindre sur le web ?

Les faux-semblants, les transactions bancaires, l'IRC, et surtout soi-même : "To know your enemy, know yourself, for you are your worst enemy".

Qu'est ce qu'être hacker et qu'est-ce qu'être un pirate ?

Etre hacker c'est aimer repousser les limites, y compris celles de la liberté, même si des fois ça doit empiéter sur celle de ceux qui nous l'offrent volontiers au détriment de ceux à qui ils la lèguent. Dans un contexte internet, je crois que la plus complète des descriptions c'est la FAQ de Eric S Raymond. Etre hacker c'est correspondre à au moins une des descriptions données dans son jargon-file, et dans un contexte réel c'est surtout la capacité à faire confiance à l'aléatoire plutôt qu'à ses règles.

Netiquette

Oui le web est un outil génial, oui on y trouve de tout, et oui on y trouve aussi des personnes sans aucune étique ni morale. Voici un courrier réel d'un webmaster qui proposait un fichier d'emails : "Je suis propriétaire d'une base de plus de 140 000 mails francophones existants et je souhaite la vendre à un webmaster désirant s'en servir pour faire la pub de son site. Une fois achetée, vous pourrez utiliser cette liste à volonté pour faire la promotion de vos services, le succès est garanti ! Ce fichier contient aucune information complémentaire comme le nom, l'age ou bien le sexe de personnes. Cette liste de diffusion est officieuse et devra le rester ! Si vous êtes intéressés par mon offre merci de me répondre assez rapidement sachant que la transaction se fera dans la plus grande discrétion..." Et les règles de base, on se les met où ? Je doute d'ailleurs que les (très nombreux) propriétaires de ces adresses apprécient l'humour. Et l'on ne parle même pas du non-respect de la loi - voir à ce sujet les articles 226-17 et 226-24 (www.cnil.fr/textes/index.htm)

David contre GOLIATH

Une société écossaise de Glasgow, Front Page Design, vient de gagner face au géant de Redmond, Microsoft, son procès sur le droit d'utiliser le nom "FrontPage". Comme vous l'aurez remarqué, le nom de cette société, qui existe depuis 1995, était effectivement très proche et les juges ont considéré, au vu de son antériorité, qu'elle y avait droit. Reste à savoir pourquoi Microsoft continue à utiliser la marque "FrontPage" au Royaume Uni sachant que celui-ci appartient à une autre société...

en bref

Microsoft négocie

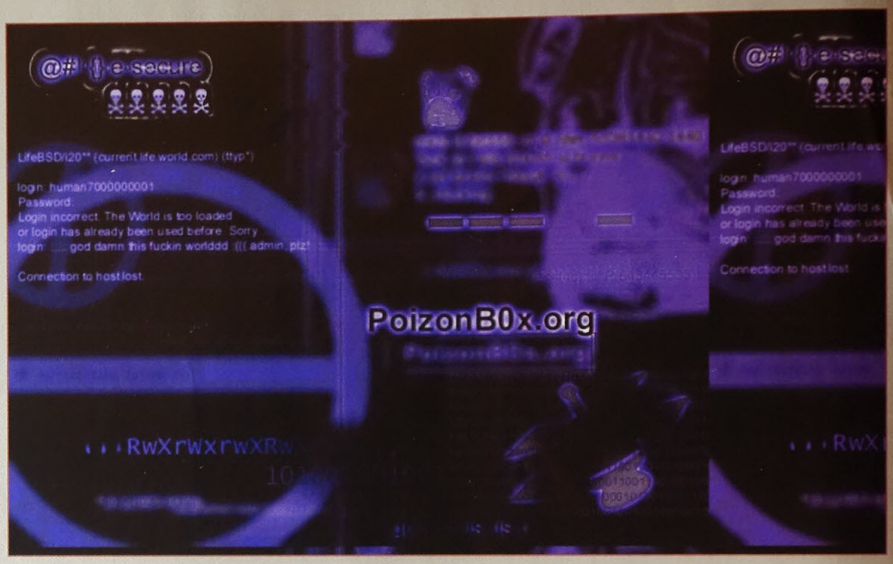
L'étau se resserre sur Microsoft sur Microsoft que les différents procureur veulent toujours démembrer. Pour lutter contre cela, Microsoft à mis au point tout un programme d'ajustements afin de pouvoir négocier dans de bonnes conditions et avoir les bonnes grâces du gouvernement. C'est du moins ce qu'a rapporté le Wall Street Journal tout en précisant que le géant de Seattle ne faisait aucune confidence sur le contenu exact de son programme… Pas facile de négocier pour Microsoft qui continue, à longueur de temps de bafouer les lois anti-trust américaines… La suite au prochain épisode !

Reconnaissance faciale contre le vol

La chaîne de libraire Borders Groups Inc. vient de suspendre temporairement l'implémentation d'un système de reconnaissance faciale dans deux de ses magasins suite à une plainte des associations de défense des droits de l'Homme. Le logiciel commercialisé par Visionics Corp compare en permanence les images des clients-consommateurs avec une base de photos de voleurs identifiés mise à disposition par la police. Quand aucun résultat probant n'est obtenu, les images sont ensuite effacées. A Londres, une initiative comparable a trouvé un terme elle aussi, pour les mêmes raisons.

Le Hacker qui aimait trop EverQuest

Les agents fédéraux ont saisi dix ordinateurs appartenant à un adolescent suspecté de piratage du jeu EverQuest. Grâce à ce piratage, le jeune homme aurait eu accès aux informations personnelles de milliers de joueurs et d'employés de Sony. Le pirate âgé de 17 ans a pu accéder à l'ordinateur du vice-président développement de Sony. Il a téléchargé certains documents ainsi qu'une version non encore commercialisée d'EverQuest… Aucune charge n'a été pourtant retenue à l'encontre du jeune homme… Coup de bol !



Hack de l'été

Juillet et août ont vu quelques 2 000 sites modifiés. Dans le lot, des sites français comme 9Telecom.fr piraté par un groupe nommé Cr1M1n4L Z0n3. Vient ensuite le serveur brésilien d'Alcatel visité par un prénommé kamikaze. C'est le 5e serveur de cette société à être visité. En mars dernier, les serveurs coréens et d'Afrique du Sud avaient été modifiés par antihackerlink et Morfeu. En novembre 2000, le serveur italien de la firme avait été barbouillé par Prime Suspectz. Dans un autre genre, le groupe pharmaceutique Pfizer a vu son site attaqué par des hacktivistes demandant que soit stopper toutes les expérimentations sur les animaux. On termine avec le serveur dédié aux professionnels de Worldonline modifié pour la seconde fois par PoizonBox...

Les eurodéputés prennent position

Le Parlement européen a du mal à trouver un terrain d'entente. C'est le projet de traité sur la cybercriminalité qui divise. Les députés européens ont adopté un avis plutôt favorable au projet. Un avis qui fera date. En effet, l'avis rappelle tout d'abord la nécessité de se prémunir contre la cyber-criminalité. Mais ce n'est pas tout car le Parlement évoque l'équilibre "entre la nécessité de faire respecter la loi et celle de préserver les droits fondamentaux et les libertés des citoyens". En d'autres termes, les données concernant les internautes ne doivent pas être conservées sans raison évidentes pour préserver le respect de la vie privée. Ainsi le délai de conservation initial d'un an vient d'être raccourci à 3 mois, conformément à ce que préconisaient les FAI. Enfin, le Parlement refuse que l'obligation soit faite aux citoyens d'ouvrir les messages cryptés et de fournir les clés de cryptage. Enfin, comme si l'Europe manquait encore d'organisations inutiles, le Parlement a conseillé la mise en place d'un forum communautaire sur la cyber-criminalité, afin que les lois soient appliquées en ce domaine. Ce forum réunirait les fournisseurs d'accès, les opérateurs télécoms et nombre d'autorités.

Le FBI pirate les sites gouvernementaux… et pénètre le milieu underground !

Grâce à une opération qui aura pris 18 mois, le FBI a mis un pied dans le milieu des hackers. L'objectif initial avoué consistait à arrêter des pirates pro-serbes courant 1999. En fait, il s'agit de la toute première action d'importance pour débusquer les hackers basés en Amérique. L'opération a mobilisé une douzaine d'agents du FBI et du Pentagone et a commencé à porter ses fruits. Pour cela, les enquêteurs ont noué des liens avec des pirates et ont eux-mêmes défacé des sites gouvernementaux pour se faire une réputation dans le milieu… Y'a plus de moralité ma pauv' dame !

Piratage Advance

Plusieurs magazines ont fait état du piratage de la Game Boy Advance, la dernière bombe de Nintendo. Un piratage grâce à un simple montage hardware à brancher sur la console. Ce n'est pas nouveau, avant même sa sortie en magasin, la console 32 bits avaient déjà été piratée grâce à des émulateurs. Nintendo avait d'ailleurs modérément apprécié la blague et avait vainement tenté de faire fermer les sites. Un émulateur de console n'a rien d'illégal. Le fait de posséder une copie du jeu au format émulation ne l'est pas non plus, à condition de posséder l'original et de ne pas mettre cette "copie" à disposition sur le Web. Attention par ailleurs aux messages d'alerte sur de nombreux sites "pirates" qui vous expliquent que vous pouvez les garder 24 heures, c'est totalement faux. Pirates et amateurs d'émulation sont des personnes différentes, même si la frontière n'est pas si éloignée. Si les premiers ne pensent qu'à se faire de l'argent sur les sociétés informatiques, les seconds sont "simplement" des fous de programmations et/ou passionnés de consoles de jeu.

Combine scientifique

Voici un paradoxe qui va faire plaisir… L'industrie ne peut empêcher la science de faire des recherches et de publier ses résultats. Le mathématicien Phil Carmody qui en mars de cette année est parvenu à encoder le source de DECSS vient de mettre au point une version exécutable du protocole de compression/décompression détesté par l'industrie du cinéma. Ces sociétés monopilistiques vont-elles une fois de plus faire pression sur les milieux scientifiques pour que ces recherches soient abandonnées ? Certainement pas car la recherche est indépendante et le public doit être tenu informé des avancées de la recherche, c'est du moins ce que les chercheurs ont objecté pour se défendre contre leurs "oppresseurs" !

Il gagne 2 millions d'euros en ligne… Le casino porte plainte pour piratage!

Les pirates s'attaqueraient de plus en plus aux casinos en ligne et en détourneraient de plus en plus d'argent. Il y a quelques jours, la société canadienne Cryptologic qui édite des casinos en ligne affirmait qu'un pirate avait cracké l'un de ses serveurs et s'était assuré que personne ne pouvait perdre. Grâce à cette manipulation, 140 joueurs ont remporté en tout 1,9 million de dollars. La brèche aurait affecté 19 casinos rattachés à la société Cryptologic. Les gains ont pu être conservés par ceux qui n'étaient mouillés dans le piratage, mais a porté plainte contre le hacker responsable de l'intrusion.

PGP à nouveau opensource

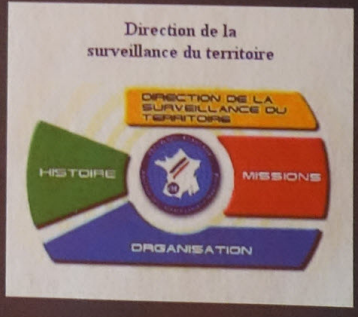
Network Advertising Initiative (NAI) a annoncé que le code source que PGP serait ouvert à la communauté. En d'autres termes, il serait de nouveau en opensource. La nouvelle a été accueillie avec enthousiasme par tous ceux qui travaillent sur la cryptographie. Même Phil Zimmermann, le créateur de PGP s'est félicité de cette initiative, précisant que NAI n'aurait même jamais dû fermer la source en première instance.

Que nous veut la DST ?

Cette fois, c'est sûr, Hacker News Magazine dérange. Comment le savons-nous ? Eh bien tout simplement parce que nous avons eu droit à la visite inopinée des fonctionnaires de la DST. Retour sur un moment troublant…

Nous sommes au tout début du mois de septembre. Dans le bureau de la rédaction, encore ensoleillé à cette heure de l'après-midi, nous entendons sonner à la porte. Aucun d'entre nous n'attendait de visite et en bons paranoïaques, nous nous penchons tout d'abord par la fenêtre pour identifier les visiteurs. Là, deux inconnus, vêtus de façon classique, plutôt décontractés se tiennent face à notre porte. Par la fenêtre du premier étage, nous les interpellons pour savoir ce qu'ils désirent. La réponse tombe comme un couperet : « C'est la police, nous aimerions vous parler ». Des mots qui glacent le sang même si l'on n'a presque rien à se reprocher. A deux nous descendons ouvrir la porte. Cette fois, c'est une carte officielle d'agent de la D.S.T qui nous attend. Les deux hommes, visiblement jeunes se présentent et nous disent n'avoir rien contre nous. « Il ne s'agit que d'une prise de contact, pour voir ce que vous comptez faire avec Hacker News Magazine… ». La question nous laisse perplexe. Avec Hacker News Magazine, nous voulons informer tout simplement. Méfiants, nous préférons ne pas les faire entrer. N'ayant pas de commission rogatoire, ils ne peuvent nous contraindre à les faire rentrer. Nous leur proposons donc un rendez-vous pour le jeudi suivant à 14 heures. Depuis, plus aucune nouvelle. Les deux hommes ne se sont pas présentés au rendez-vous, n'ont pas rappelé, ne sont pas passés nous voir.

Alors, chez nous, les questions fusent… S'agissait-il de véritables agents de la DST ? Si oui, que voulaient-ils exactement ? Leur démarche n'est pas claire. S'il ne s'agit pas de vrais agents, par qui étaient ils envoyés ? Honnêtement tout est possible, mais en attendant, au sein de la rédaction la méfiance et la parano ont atteint leur paroxysme. Mais nous ne manquerons pas de vous tenir au courant des prochains épisodes du feuilleton "La DST veut connaître Hacker News Magazine"…



en bref

Travail : méfiez-vous de vos collègues

Chaque bureau aurait son hacker, c'est ce qu'affirment des experts en sécurité. IBM ne manque pas d'utiliser ces annonce pour refourguer son module sécurité E-business. Une association d'industriels anglais a annoncé il y a quelques temps, que les deux tiers des entreprises anglaises avaient été victimes d'incidents informatiques provenant de l'intérieur (attaques virales, fraudes etc.). De nouveaux marchés semblent s'ouvrir pour les éditeurs de solutions de sécurisation.

Les ricains embauchent les hackers

Le gouvernement américain cherche désespérément à embaucher des hackers. Ils viennent de recruter un ingénieur à la retraite de 63 ans, une mère de famille et un jeune homme aux cheveux longs pour recruter ces pirates. Une bourse est même proposée. Un budget de 8,6 millions de $ pour offrir deux ans de formation à des hackers contre deux ans de service dans les administrations a été débloqué. C'est sûr, ils nous aiment !

Pas si sûr...

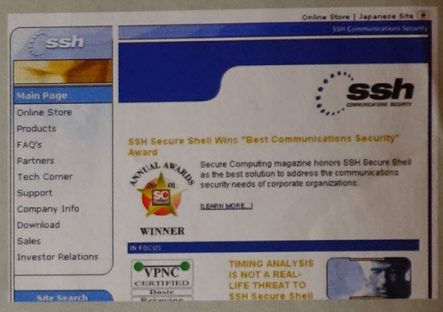
Selon le Secrétaire à la Défense américain, la plus grosse menace de ce début de XXIe siècle (hormis Ben Laden) serait le cyber-terrorisme. Et ce dernier préconise la tolérance zéro. Il pense donc réformer tout le système de défense américain afin de l'orienter vers la traque et la lutte contre le cyber-terrorisme. Ce gentil monsieur estime que comme les terroristes ne peuvent lutter à armes égales avec les USA, ils se tournent d'instinct vers l'arme informatique... Hé garçon, maintenant qu'il pleut des Boeing sur New-York, t'es toujours sûr que la plus grosse menace, ce sont les hackers ?

Histoires chinoises

Une étude sur l'usage domestique de l'informatique révèle que la moitié des internautes chinois se seraient plaint d'avoir été victimes de hacking et de piratage l'an dernier. Selon cette étude, ce chiffre élevé est dû au peu de précautions prises. Alors qu'un nombre croissant de hackers est estimé en Chine, il apparaît que les Chinois sont les moins bien informés en matière de sécurité.

Achetez en toute insécurité!

Les chercheurs en matière de cryptographie ont identifié une faille au sein de Secure Shell. Cette faille permettrait aux hackers d'obtenir des informations sur les mots de passe utilisateurs. Les informations supplémentaires qui pourraient être interceptées concerneraient notamment le trafic sur le site, les temps passés sur chaque page, etc. Dommage pour des champions de la sécurité...



DANGER : la France veut battre la Chine en termes de restriction des libertés !

Contrairement aux promesses faites début 1999, le Projet de Loi sur la Société de l'Information (LSI) (www.assemblee-nationale.fr/projets/pl3143.asp) ne contient pas un article unique abrogeant toutes les dispositions actuelles de la législation française consacrées à la cryptographie. A l'inverse, le Projet LSI a fait le choix de définir et réglementer ce domaine de l'informatique et du savoir (l'enseignement de la cryptographie est aussi concerné) :

```
Article 36
On entend par moyen de cryptologie tout matériel ou logiciel conçu ou
modifié pour transformer des données, qu'il s'agisse d'informations
ou de signaux, à l'aide de conventions secrètes ou pour réaliser
l'opération inverse avec ou sans convention secrète.
```

Selon le Projet de LSI, l'usage de cryptographie devient libre mais... la "fourniture" de cryptographie est sévèrement limitée ! Pour des raisons hélas trop connues (les écoutes téléphoniques administratives), depuis 1939 la France interdisait l'utilisation libre de cryptographie. Elle constituait une exception regrettable au milieu des autres grandes démocraties et c'est cette exception que M. Lionel Jospin avait voulu lever en 1999 en décidant la libéralisation complète de la cryptographie.

Deux ans après, le Projet de Loi sur la Société de l'Information n'abroge pas les réglementations visant la cryptographie ; pire, il définit la notion de "cryptologie", et crée des limitations à la liberté d'expression fondées sur un hypothétique danger que feraient peser sur la société les programmes de cryptographie. La fabrication et la fourniture de couteaux de cuisine est libre, mais la libre écriture et la libre diffusion de logiciels informatiques de cryptographie est interdite !

Légiférer sur la cryptographie est dangereux pour les libertés fondamentales (notamment la liberté d'expression et la liberté d'opinion). Si la LSI était votée en l'état, vous ne pourriez plus diffuser librement les trois lignes de script PERL qui suivent puisque cela constitue une "fourniture" d'outil de cryptographie (avec algorithme RSA) :

```
#!/bin/perl -Chiffrement-RSA-en-3-lignes-de-langage-PERL
-sp0777i<X+d*lMLa^*lN%0]dsXx++lMlN/dsM0<j]dsj
$/=unpack('H*',$_);$_=`echo 16dio\U$k"SK$/SM$n\EsN0p[lN*1
lK[d2%Sa2/d0$^Ixp"|dc`;s/\W//g;$_=pack('H*',/((..)*)$/)
```

Légiférer sur la cryptographie est inutile. Si quelqu'un veut se protéger d'une écoute administrative, ce n'est pas l'interdiction de diffusion de la cryptographie qui l'en empêchera : on trouve de la crypto forte, gratuite et facile à utiliser, partout sur Internet, et les logiciels libres GNU GPL comme Linux (complètement ignorés par le Projet LSI) en accélèrent la prolifération de jour en jour. Légiférer sur la "cryptographie", c'est chercher à capturer le vent ; c'est stupide : à la fois inutile et dangereux.

"Le droit de parler le PGP est comme le droit de parler le Navajo. Le gouvernement n'a aucun droit spécifique de vous empêcher de parler d'une manière technologique, même si c'est plus compliqué pour lui de comprendre ce que vous dites." (Eben Moglen, professeur de droit, Université de Columbia, New York).
www.geocities.com/openpgp

le CPCNG le futur de l'ordinateur est peut-etre

>>> "Et si on créait un nouvel ordinateur ?" Si l'histoire du CPCNG commence comme une boutade, la suite prouve que le projet en a intéressé quelques-uns. Depuis la petite annonce dans le magazine les "Puces Informatiques", les deux Christophe (Christophe Guelff et Christophe Dupas) ont développé une véritable synergie autour de ce projet : lancer l'idée folle de créer un ordinateur pas cher et libre.<<<

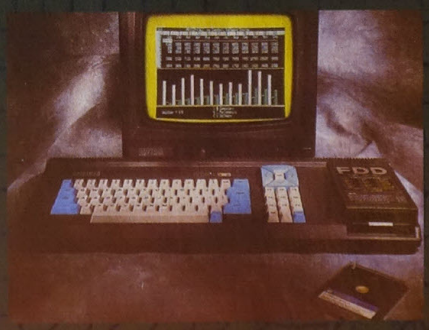
LIBRE

l'Ordinateur libre

Si l'idée en elle-même n'est pas nouvelle dans la tête de Guelff, le CPCNG ne se développe pourtant que depuis quelques mois maintenant. Architecturé autour d'un processeur E-Z80 de la société Zilog (**http://www.zilog.com**), ce nouvel ordinateur devait être, dans un premier temps, le successeur de l'Amstrad CPC. Depuis, les discutions houleuses autour de cette compatibilité ont permit de recentrer les développements sur des possibilités du E-Z80. Sans remettre en question la disponibilité des logiciels tournant sur l'Amstrad, le CPCNG s'oriente à présent sur des applications beaucoup plus viables.

« Networks Computers », le mot est lâché. Marchant dans le sens des technologies de demain, le CPCNG devrait être un terminal directement relié sur le net. Un disque dur à Tokyo, un traitement de texte en Arabie Saoudite, l'avenir nomade est plus que certain et le CPCNG reposera pour une grande partie sur le fait que les données pourront être accessibles directement depuis sa connexion à Internet. Une société pourrait très bien proposer un tel service sur le réseau, rendant ainsi possible une sorte de location d'espace disque.

L'utilisation en tant qu'ordinateur familial est aussi privilégié, connexion sur Internet, traitement de texte, tous cela est d'actualité. C'est d'autant plus probable que la disponibilité de Linux sur le hardware du CPCNG est route. En effet, le projet est à présent référencé sur le site de linux.org. Les utilisateurs devraient donc avoir accès à la logithèque impressionnante du célèbre OS libre. Car si le processeur n'est pas un "monstre" de puissance (sa fréquence d'horloge n'est que de quelques 50 MHz), l'équipe compte mettre en avant les possibilités "réseaux" du



cœur du CPCNG. Protocole TCP/IP, http, FTP sont des fonctions intégrées à l'E-Z80. Le bébé de ZILOG est, peut-être bien, le noyau des futures appareilles informatiques. Téléphones, PDA, station Internet, tous ce qui pourrait donc être d'une façon ou une autre connecté à un réseau est susceptible d'utiliser ce processeur. La conception du E-Z80 est depuis le début orienté vers l'avenir, vers le "tous réseaux".

Si le choix de l'équipe s'est porté sur ce processeur, c'est d'un coté pour l'image de ZILOG dans l'informatique des années 80, mais aussi parce que le prix du principal composant du CPCNG ne devrait pas dépasser les 15 Euros (Moins de 100 FF). Si la politique suit, le coût de revient pour se faire son CPCNG à la maison n'explosera pas les budgets. Pour moins de 250 Euros, un particulier possédant des connaissances suffisantes en électronique devrait parvenir à se créer son propre CPCNG, juste avec un fer à souder et quelques composants électroniques. Pas de panique si le bricolage est une compétence qui vous fait défaut, en prenant votre mal en patience il est très probable qu'une « distribution » basé sur le CPCNG sortira en parallèle. D'un concept similaire à celui qui fait le succès de Linux actuellement, le CPCNG est un ordinateur libre. Que ce soit un particulier ou une société, l'exploitation de l'ordinateur est possible, même pour un usage commercial. Seules contraintes, les modifications apportés devront, elles aussi, être libres et utilisables par d'autres, et la compatibilité entre les ordinateurs ne devra pas être remise en question. Les deux équipes sont à présent sur une ligne droite. L'équipe hardware va attaquer, dès la disponibilité du E-Z80, le premier prototype. L'équipe software n'est pas en reste et compte bien terminer le premier émulateur tout en mettant les premières fondations à l'OS et à sa compatibilité avec le CPC. Tous cela devrait aller très vite, l'équipe, regroupée autour de l'association Cocoon System (http://cocoonsystem.free.fr), compte des personnalités comme Hans Summers, Kevin Thacker (créateur de l'émulateur Arnold) ou Stefan Stumpferl (du futur OS, le system d'exploitation alternatif pour Amstrad). De plus, Roland Perry (le créateur du CPC chez Amstrad) pourrait venir donner son expérience et ses conseils afin d'aider la toute jeune équipe.

Si les objectifs sont respectés, d'ici l'année prochaine, les premiers prototypes seront en test. L'équipe promet une surprise pour ce printemps. Faudra encore avoir assez de patience pour attendre jusque là. Mais si vous pensez posséder assez de motivation pour vous lancer dans l'aventure avec eux, rien ne vous empêche de vous rendre sur le site et de vous abonner à la mailing liste. Le groupe recherche de nouvelles compétences et espère bien recruter de nouvelles personnes motivées par l'aventure extraordinaire du CPCNG. Il y-a peu de temps, un sondage à permis de constater que des dizaines de personnes serait prêt à préacheter des CPCNG. **Et vous ?**

defcon

DEF CON

>>> Pour la 9ème année consécutive Las Vegas a accueilli le DEF CON, rassemblement de bidouilleurs, informaticiens, hackers et autres pirates venant chercher un peu de sensations fortes dans ce meeting pas comme les autres. <<<

9

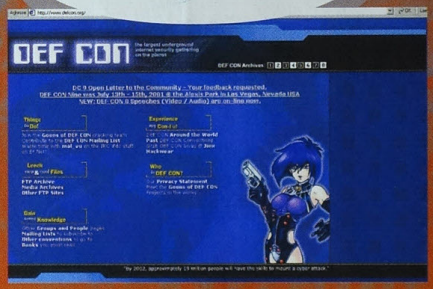
Le Defcon est connu pour être le meeting de « hackers » le plus exubérant du monde. Aussi connu pour son contenu technique que pour ses buveurs de bière et tireurs fous. Cette année le Defcon a été plus sage, plus propre encore que l'année dernière.

Un tract anonyme a d'ailleurs reproché cet état de fait. Il notait justement cette rentrée dans le rang, et aussi, le fait qu'il ne fallait pas payer l'entrée au Defcon. Une entrée bien gardée par des gros bras derrière leurs barrières en fer regardant les badges-pass avec un certain zèle. On se serait presque cru à l'entrée de Loft Story. La presse a eu droit à ses conférences quotidiennes sans compter le petit document de deux pages, à signer, obligeant les journalistes à respecter certaines règles. Pas de photos par exemple. Juste un détail, les organisateurs ont-ils fait signer les dirigeants de l'hôtel pour les obliger à crypter les visages filmés avec les caméras de vidéos surveillance ?

Le laisser-faire du début a pris aujourd'hui une autre tournure, plus pro. Les participants semblaient plus vieux cette année, sur un peu plus de 5 000 participants/visiteurs un tiers seulement semblaient avoir moins de 21 ans. Le professionnalisme de ce rassemblement a agacé quelques-uns des participants, le tract déjà cité en est l'une des preuves. Appeler à la désobéissance à l'encontre de l'organisation du Defcon, il fallait oser. "Don't pay for DC registrations ... steal a badge ... reclaim your culture ... hack the exploiters ... ignore the rules ... don't buy anything." Ne payez pas l 'entrée, volez des badges, ignorez les règles, n'achetez rien, ...

> Les conférences

Côté info, de belles conférences, celles de Bruce Schneier, l'auteur James Bamford, etc... Côté technique, un point fort au sujet des réseaux sans fil, 802.11. A noter qu'IBM annonçait au même moment la sortie d'un logiciel qui veille sur les transmissions sans fil. Il se nomme Wireless Security Auditor, il s'adresse aux administrateurs de réseaux sans fil, basés sur la norme de transmission 802.11. " Un hacker qui se promène dans le quartier en voiture, ou qui se gare sur un parking, peut facilement se connecter au point d'accès 802.11 pour attaquer l'entreprise et espionner ses e-mails, par exemple ", a reconnu Dave Safford, le



responsable de la sécurité des réseaux chez IBM Research. Le logiciel vérifie que les données ne sont pas interceptées sur le réseau de l'entreprise. Côté lecture, la partie livre de la mort qui tuent avec par exemple " Comment se cacher dans un endroit public " " Lire sur les lèvres " ou encore " Vous et la Police ".

C'est la première année que le CdC, Cult of the dead Cow, ne faisait pas un vrai show comme ils en ont le secret. En 1998, il avait défrayé la chronique avec le trojan Back Orifice, en 1999, même scénario avec Back Orifice 2000, qui n'était plus un virus de Troie mais un outil d'administration à distance. Cette année, le CdC devait sortir Peekabooty, un navigateur qui doit permettre de surfer dans l'anonymat. Un logiciel destiné aux internautes de pays totalitaires. Les informaticiens qui planchent sur Peekabooty ne le considéraient pas suffisamment au point pour le présenter. Ce programme est de type peer-to-peer comme Gnutella ou Napster. Rajoutez-y une pincée de Freenet et le tour est presque joué car il reste quand même le doigté de ce groupe mythique. Le groupe, Le culte de la vache morte, CdC, est connu pour avoir mis en service le plus connu des virus trojan, Back Orifice, il explique dans son communiqué "Qu'il serait irresponsable de libérer le logiciel dans son état actuel."

> A suivre !

Le Black Hat, qui se tient toujours une semaine avant le Defcon a regroupé quant à lui 1300 pointures de l'informatique. Administrateurs de grosses sociétés, membres des forces de l'ordre, créateurs de logiciels, dont certains français. Un projet a été annoncé durant ce Black hat : Le Honeynet Project. En bon français, ça donne le pot de miel. L'idée est simple, mais pas nouvelle. Un groupe d'une trentaine de professionnels de la sécurité va s'attaquer à suivre les méthodes, outils et techniques utilisées par les pirates. Pour cela, vont être mis en place de faux sites, de faux serveurs afin de piéger les abeilles, ou plutôt les pigeons. Le prochain Black Hat doit se tenir mi-novembre en Hollande. Même prix d'entrée, 1095 dollars.

En parlant des forces de l'ordre, un débat qui a marqué les esprits, surtout à la fin de la conférence nommée : "Meet the Fed" tenue par le FBI, un membre du Congrès Us et des experts en matière de sécurité. Jim Christy, un agent spécial de la surveillance pour le service de la défense y a diffusé sa carte de visite comme des petits pains. "Il y a un tas de talents ici - mettons ce talent à bonne contribution". Le débat a duré une heure, l'après débat entre les fédéraux et les " hackers " aura durée presque deux fois plus.

> Direction case prison

On termine avec l'arrestation d'un russe, quelques heures après le Defcon. Son crime est d'avoir présenté un moyen de contrer la sécurité mise en place par Adobe Software. Dmitry Sklyarov, ingénieur de 26 ans, a donc parlé de « la sécurité des ebooks, théorie et pratique », le problème est qu'il sera arrêté dans sa chambre d'hôtel par le FBI, le 16 juillet, quelques heures après le Defcon. Il sera accusé d'avoir trouvé le moyen de copier et imprimer les documents ebook protégés par le système d'Adobe. Le cryptographe russe tombait sous le coup de la loi sur le Copyright Us, la « très » controversée Digital Millenium Copyright Act. Le FBI ne manquant par d'humour, appellera cette arrestation "Travesty".

Dmitry Sklyarov sera relâché le 6 août, sous caution, après une série de manifestation devant les locaux d'Adobe et une avalanche de courriers électroniques, des actions lançaient par l'Electronic Frontier Foundation, qui tente de défendre la liberté d'expression sur l'internet.

Le site officiel du Defcon
http://www.defcon.org
site Honeynet
http://www.honeynet.org/
Cult of the Dead Cow
http://www.cultdeadcow.com/

La panoplie du parfait 007

>>> La fin de la Guerre froide n'a pas signé l'arrêt de mort de l'espionnage… Qu'ils soient industriels, politiques ou tout simplement d'ordre privé, les motifs ne manquent pas! Surtout de nos jours, alors même que la technologie moderne offre de nombreux terrains de jeux aux apprentis James Bond. Grâce à Internet, notamment, n'importe qui peut quasiment se procurer n'importe quoi, malgré une législation française sourcilleuse. Démonstration…

Souvenez-vous, grâce à une paire de lunettes, il pouvait filmer une conversation… Avec un simple étui à cigarettes, il était capable de prendre des photos ou d'ouvrir une porte… Tous ces gadgets chers à James Bond, sortaient souvent de l'imagination fertile de scénaristes. Et pourtant… la plupart d'entre eux existent bel et bien, ou ont existé… Oh, bien sûr, on ne parle pas de la Lotus Esprit amphibie qui relève plutôt de la science-fiction… Non, il s'agit de tous ces accessoires capables de transformer le moindre curieux en parfait 007. Les films de James Bond ont-ils inspiré les ingénieurs spécialisés dans la surveillance ou est-ce le contraire? Cela revient à se poser la fameuse question existentielle: qui a commencé, de l'œuf ou la poule? Qu'importe, les faits sont là…

Les objets de la vie courante se transforment vite en gadgets-espions car c'est encore le meilleur moyen pour les rendre discrets. «Discret», c'est le mot consacré lorsque l'on parle d'espionnage, - ou de surveillance pour rester dans le politiquement correct. Le mot d'ordre est largement respecté… Par les officiels

La panoplie du parfait 007

Le Web au service de l'espionnage

Quant aux privés, ils ne sont pas épargnés: la loi sanctionne sévèrement les apprentis-espions lorsqu'ils ne respectent pas suffisamment les règles. Enfin, la discrétion s'applique également aux magasins chargés de distribuer toutes ces merveilles de la technologie; ils ont rarement pignon sur rue! Se procurer un gadget relevait auparavant de la mission, sinon impossible, en tout cas difficile. C'était avant que les frontières ne soient virtuelles… Aujourd'hui, avec le Web, la technologie est au service d'une autre technologie, celle de l'espionnage. Les sites existent, il faut juste les connaître, et respecter les conditions qu'ils préconisent. Bienvenue dans le monde du «voir sans être vu».

Nous n'irons pas jusqu'à dire que le matériel de surveillance est disponible à chaque coin de rue d'Internet, ce serait exagéré. Il faut quand même les dénicher car ils s'entourent de multiples précautions juridiques. En France, l'utilisation du matériel de surveillance est très réglementée, la plupart des appareils sont interdits (lire encadré consacré à la législation). Certains d'entre eux sont autorisés à la vente mais il est interdit de les utiliser: c'est l'éternelle rengaine de l'hypocrisie…

«Mais oui monsieur, vous avez parfaitement le droit d'acheter ce micro-espion, mais vous n'avez pas le droit de l'utiliser, ou alors pour enregistrer vos propres conversations… Bien sûr, les gens avec qui vous discutez ne doivent pas être écoutés à leur insu, ils auront préalablement été prévenus… Voilà, monsieur, bonne écoute!» Ainsi, les commerçants ne manqueront de vous prévenir que certains appareils ne doivent pas être utilisés à des fins «d'espionnage». Quant aux matériels qui ne sont pas commercialisés en France, même hypocrisie, ils sont vendus dans des pays frontaliers, par l'intermédiaire de sites traduits en français! Ces précisions expliquent pourquoi, lorsque vous effectuez une recherche sur le Web, vous trouvez des sites franco-français et des sites hébergés à l'étranger, dans des pays où la législation est plus «souple».

Autorisés ou non, les gadgets ne manquent pas: toute la panoplie du parfait espion est disponible. Si vous êtes une cible privilégiée en matière de concurrence industrielle ou à titre privé, vous pouvez en savoir plus grâce au Web sur les méthodes d'espionnage et le matériel utilisé. Nous parlerons d'abord de tout ce qui concerne l'écoute, par l'intermédiaire de micros-espions ou sur une ligne téléphonique, ensuite nous évoquerons les matériels d'observation, et à chaque fois, les parades les mieux adaptées seront présentées. Enfin, nous terminerons par ce qui est insolite…

La transmission et les micros-espions

Les micros-espions sont vendus librement mais il est - évidemment - interdit d'écouter une conversation à l'insu des interlocuteurs… Ainsi, les sites qui proposent ce type de matériel vous indiquent que ces micros serviront à la «surveillance d'habitations, ou de locaux professionnels, levée de doute en cas de vol ou d'agression, surveillance et écoute permanente de bébé...»

Par ailleurs, les sites français précisent bien qu'il est interdit d'acheter ces produits sans «une demande préalable auprès des autorités compétentes». C'est le cas de Prodels.com qui bénéficie d'un catalogue assez complet. La plupart sont des micros HF à fréquences auto-compensées, des émetteurs… En clair, ils émettent un signal sur une fréquence prédéterminée et il suffit d'un simple transistor ou d'un autoradio, pour écouter ce signal. La capacité de certains d'entre eux est impressionnante, avec une antenne adéquate, la portée peut atteindre une dizaine de kilomètres!

Le micro-espion classique se présente sous la forme d'un petit appareil, à peine plus grand qu'une pièce de monnaie, il est alimentée par une pile 9 volts et peut se dissimuler n'importe où dans la pièce d'une habitation: son autonomie est de plusieurs jours, sa portée peut atteindre plusieurs centaines de mètres et son prix se situe aux alentours de 200F. Dès que le matériel prend une forme plus commune, ressemble à des objets de la vie courante, le prix monte…

Exemple, ce micro prise-téléphone: microphone HF haute sensibilité raccordé directement sur la prise téléphonique (écoute exclusivement les bruits de la pièce). Il se présente sous la forme d'une prise téléphonique double sur laquelle vous pouvez brancher 1 ou 2 équipements téléphonique. L'émission est permanente et l'autonomie illimitée. La fréquence d'émission est située en dehors de la bande publique et ce gadget coûte

Une législation française sans pitié

Que de nombreux gadgets soient en vente libre oui non, ou que l'on puisse se les procurer facilement; c'est un fait… Pourtant, la loi française est sans pitié pour les apprentis-espions. Tout d'abord, l'article 9 du Code civil mentionne que «chacun a droit au respect de sa vie privée…». Cette simple phrase concerne les écoutes, la surveillance vidéo, ou simplement des photos. La personne qui est espionnée à son insu peut porter plainte et obtenir des dommages et intérêts.

Par ailleurs, il en est de même pour un patron qui ne peut surveiller ses employés à leur insu, grâce à des caméras, et ce en vertu des articles L 121-8 et L 120-2 du code du travail. De plus, et fort heureusement, de tels enregistrements vidéo n'ont pas de valeur devant les juges. Il en va de même pour l'enregistrement de paroles échangées à titre privé dans votre vie professionnelle, en vertu des articles 226-1 du code pénal et 9 du code civil.

Enfin, si quelqu'un s'introduit chez vous pour y poser des micros, la violation d'un domicile est punie par 100.000F d'amendes et 1 an de prison (art. 226-4 du code pénal). Concernant les procédés d'enregistrement vidéo des lieux privés ou de captation des paroles non publiques, l'auteur risque 300.000F d'amendes et un an de prison. Comme nous l'avons évoqué dans ce dossier, la plupart des gadgets présentés sont interdits… Ils sont commercialisés (parfois sans autorisation), mais il est interdit de les utiliser! C'est donc le cas de tout ce qui concerne les écoutes-téléphoniques, micros-espions, etc-, en vertu des articles 226-15 et 226-1 du Code pénal. Avant d'utiliser tous ces matériels, il faut demander une autorisation au ministère de la Défensemais nous ne pensons pas que le souhait d'écouter les secrets de famille de votre belle-mère soit un motif valable. En effet, «le matériel audio est soumis en France métropolitaine et territoires outre-mer, par la loi du 10 juillet 1991 et aux articles 226-1 & R 226-1 et suivants du code pénal. Toutes acquisitions, détentions et utilisations sont soumises à une autorisation ministérielle délivrée par la SGDN.» Pour obtenir ce numéro d'acquisition, il faut vous adresser au: Secrétariat Général de la Défense Nationale - 51 Bld de la Tour Maubourg - 75700 Paris Cedex 07 SP.

A bon entendeur…

La panoplie

environ 500F. Dans votre bureau, quelqu'un de mal intentionné remplace la prise de vos téléphones (elles se ressemblent toutes!) et vous voilà espionné!

Autre exemple, original celui-là, un micro-horloge! Il se présente sous la forme d'une banale horloge murale à aiguilles qui dissimule un microphone HF haute sensibilité. La fréquence de l'émission est réglable par l'utilisateur et la portée peut atteindre quelques centaines de mètres même en zone urbaine. Ce microphone est alimenté par une pile de 9 volts qui lui procure deux semaines d'autonomie en émission permanente. Une horloge qui donne l'heure et... éventuellement des informations: méfiance!

> Un micro caché dans un stylo

Les micros-espions les plus performants se présentent sous la forme d'un boîtier de la taille d'un paquet de cigarettes, ils sont très sensibles et leur portée peut atteindre plusieurs kilomètres. Comme pour beaucoup de ces matériels, les espions rivalisent d'imagination pour «habiller» ces micros dans les objets les plus banals: lampes, sous une table... Ouvrez l'œil!

D'autres font encore plus fort, comme **Crelec.com**, qui commercialise - toujours à l'attention de ceux qui ont l'autorisation-, des micros-émetteurs dissimulés dans une calculatrice ou dans une prise de courant multiple et pilotés par quartz. Des objets originaux pour surveiller un bébé!... Encore plus fort, et toujours vu sur le Net (cb-security.com), des micros-espions sous la forme d'un cendrier ou, plus pratique, d'un stylo tout simple. Ce dernier accessoire est digne de James Bond!

Il y en a d'autres, plus modernes, dont il faut se méfier... Le téléphone portable, notamment, est très à la mode. Celui-ci est un peu spécial, il ressemble à un téléphone portable de type GSM Ericsson. Il fait bien sûr office de téléphone mais il est également équipé d'un micro-espion... Si une personne mal intentionnée vous le prête, vous ne verrez rien... Par contre, si son propriétaire compose - n'importe quand - un numéro spécial, où qu'il soit dans le monde, le micro se met en mode émission, et à l'autre bout du fil, il entend tout ce qui se passe dans la pièce. Il existe même une version permettant d'écouter les conversations téléphoniques émises ou reçues!

Alors, avant d'accepter un portable comme cadeau, réfléchissez à deux fois! Ce gadget que 007 ne manquera pas d'utiliser dans un de ses prochains films - actualité oblige -, a été vu sur un site espagnol qui possédait auparavant une version française... Depuis peu, ce site a cessé ses ventes à

destination des Français pour des questions légales... Devant le succès du site traduit en français, les autorités hexagonales se sont-elles inquiétées de la fréquence des échanges franco-espagnols? C'est probable... Il existe toujours le site espagnol de **Secret.Uni-Dev.som** et nos voisins ne manquent pas non plus d'imagination... La preuve avec ce téléphone portable qui n'est pas le seul accessoire disponible...

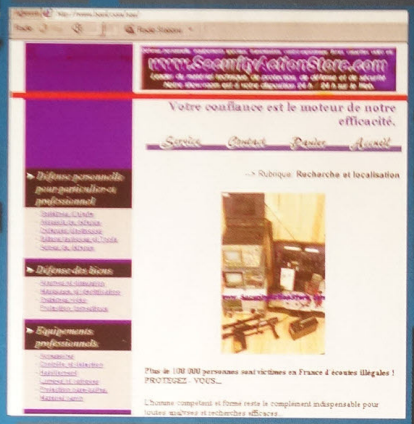
En plus des traditionnels micros-espions sous toutes leurs formes, les commerçants ibériques proposent un gilet bien particulier. Ce «kit de vigilance» a été conçu pour la communication secrète et il se compose d'un gilet sans manche équipé de nombreuse poches. Dans les poches: un micro et tous ses accessoires qui permettent de le faire fonctionner, batterie, bobine... Pour déclencher l'émission, le propriétaire dispose d'un interrupteur spécial dans la main. Il est difficile de savoir que votre interlocuteur est ainsi équipé sous sa chemise!

> Plusieurs moyens de contre-espionnage

Comment se protéger? Il existe plusieurs moyens de contre-espionnage, plus ou moins coûteux... Si une pièce est équipée de micros-espions, avant d'essayer de les trouver, vous pouvez brouiller l'écoute grâce à des appareils qui émettent une sorte d'ultrason. Le résultat pour la personne qui écoute est un effet «Larsen» très gênant (**SecurityActionStore.com**, env. 7000F). L'appareil en question sert aussi bien contre une écoute téléphonique que contre les micros-espions.

Plus simple si vous n'avez pas de brouilleur sous la main: le bon vieux coup du robinet que l'on voit dans tous les films d'espionnage... Hé bien, c'est efficace: vous laissez couler un robinet dans la pièce et ce brouhaha couvre votre conversation. C'est un bricolage qui s'avère économique. Pour ceux qui souhaitent investir, l'idéal est d'avoir recours à du matériel de haute technologie comme une valise de détection... Elle peut tout faire: détecter des micros-espions, contrôler des lignes

La panoplie du parfait 007



www.SecurityActionStore.com Les sites français mettent davantage l'accent sur le contre-espionnage, il faut dire que la législation est sourcilleuse.

téléphoniques et éventuellement détruire les matériels ennemis. L'attaché-case de James Bond! Ce «joujou» a un prix, comptez environ 60.000F (**SecurityActionStore.com**). C'est le prix de la sécurité mais à ce tarif là, il faut vraiment en faire son métier, sinon, il est préférable d'appeler des professionnels et de leur demander de «nettoyer» votre local durant une journée.

Vos concurrents ou voisins peu scrupuleux peuvent aller plus loin que la simple écoute par l'intermédiaire de micros-espions, vos conversations téléphoniques sont des proies de choix. En France, les écoutes téléphoniques sont réservées aux pouvoirs publics (police, services de renseignement…) et elles sont de plus en plus nombreuses d'après les statistiques. Les écoutes sauvages sont, elles aussi, en recrudescence, le fait d'être interdites n'empêche pas les «privés» d'en faire usage.

Il y a deux façons d'espionner des communications téléphoniques: en installant un micro-espion au niveau du téléphone visé ou en piratant directement la ligne. Les micros sont très performants et ils se présentent sous plusieurs formes; un microphone qui se fixe sur l'appareil téléphonique et capte le son par induction, sans avoir besoin de se connecter sur le fil téléphonique; ou un condensateur qui se connecte directement sur la ligne et ne dérange pas la fonction du système téléphonique (de 100 à 300F environ, sur le site québécois de **Safecommunication.com**). Si vos espions ne veulent pas être démasqués facilement, ils se connecteront directement sur votre ligne grâce à des adaptateurs ou des relais téléphoniques qui se présentent sous la forme de boîtiers plutôt discrets. Ils sont apparemment installés au niveau des centraux intercom et ils permettent d'enregistrer toutes les conversations (**Crelec.com**).

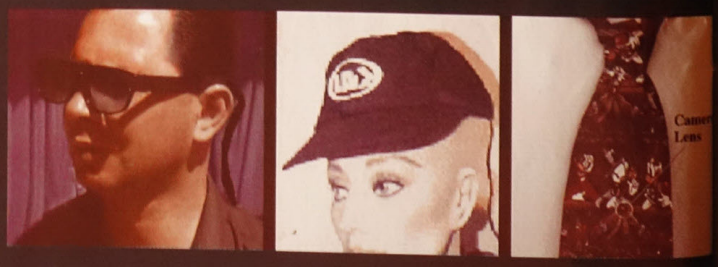
> Une caméra dans une paire de lunettes

Là encore, que ce soit pour les micros ou les boîtiers, la fameuse «valise» dont nous avons déjà parlé sera capable de détecter une éventuelle écoute. Vous pouvez aussi, faire appel aux brouilleurs qui font double-emploi: micros et téléphone. Le nec plus ultra reste l'analyseur de spectre, c'est un engin conçu pour visualiser sur son écran l'ensemble des transmissions radio-électriques (écoute d'ambiance, micro-espion, écoute téléphonique, transmission vidéo...); l'arme fatale contre toutes les écoutes pour la «modique somme» de 78.000F environ (**SecurityActionStore.com**). Il faut vraiment en avoir besoin! D'autant que l'analyseur de spectre est loin d'être discret; rien à voir avec un paquet de cigarettes ou une valise, c'est un gros appareil électrique, encombrant et voyant. La miniaturisation a beau faire des progrès, il y a des limites… Un appareil de contre-espionnage performant a besoin d'un minimum de puissance pour être efficace.

Dans un bon film d'espionnage, le son est donc important, mais il y a un autre paramètre indispensable: l'image! Vous étiez - peut-être - écoutés… Souriez, vous êtes filmés! Numérique, ondes hertziennes, laser… La technologie actuelle offre aux ingénieurs-concepteurs un large champ d'action en terme de vidéo. Avec fil, sans fil, faisceau laser, vidéo HF… Les espions ont l'embarras du choix. Leur matériel préféré: la transmission vidéo à distance sans fil. Un minimum de mise en place et une discrétion sans pareil. L'installation la plus simple et la moins onéreuse est le principe de transmission FM, il suffit d'un boîtier émetteur vidéo miniaturisé relié à une caméra. Le transmetteur peut être dissimulé n'importe où, dans un meuble ou une plante verte; sa taille peut être inférieure à un paquet de cigarettes. La portée varie en fonction de la puissance, entre 100 et 4000 mètres. Il suffit ensuite d'un récepteur et d'un écran pour visualiser les images. Un jeu d'enfant! Mais l'aspect le plus intéressant demeure l'optique. Les caméras ont réduit leur taille et c'est vraiment impressionnant! **Crelec.com** propose une caméra qui ne dépasse pas la taille d'une pièce de 5 francs (29X29X13 mm). Le capteur CCD dont elle est équipée lui permet une résolution exceptionnelle et elle pèse 20 grammes. C'est dire les nombreuses applications qu'elle peut avoir. La dernière née mesure 14mm sur 14 et elle fonctionne en noir et blanc… Où s'arrêteront-ils! Du côté des trouvailles originales, **SecurityActionStore.com** a pensé à installer une caméra miniature dans un livre apparemment inoffensif. Il se range dans une banale bibliothèque et rien ne lui échappe.

www.SafeCommunication.com Sur Internet, les québécois sont à la pointe de l'espionnage en matière de technologie; est-ce dû à la proximité des USA?

Pourtant, le terrain de jeux préféré de James Bond reste le Québec (**Safe Communication.com**)… Nos cousins d'outre-Atlantique ont installé des caméras miniatures dans des objets de la vie courante comme une paire de lunettes de soleil, une cravate, une casquette… C'est spectaculaire, votre interlocuteur devient un véritable studio vidéo ambulant et on ne voit strictement rien!



Pour les caméras miniatures, il faut compter entre 1000 et 3000F… Pour les lunettes de soleil par exemple, comptez quand même 25.000F.

Heureusement, là encore, il existe des parades… Pour contrôler une pièce sans faire appel à la fameuse «valise de détection» très

La panoplie du parfait 007

onéreuse (60.000F), optez pour un fréquencemètre capable de détecter tous les émetteurs, qu'ils soient audio ou vidéo (environ 2600F, SecurityActionStore.com). Si ce n'est pas suffisant, prévoyez la «grosse artillerie», un détecteur haute-performance qui peut déceler à distance tous les circuits électroniques, même inertes (155.000F! **SecurityActionStore.com**).

Se fabriquer une nouvelle identité

Ainsi, vos concurrents peuvent vous observer facilement, sans être vus, ou sans que vous vous en doutiez. Et si les caméras ne sont pas suffisantes, il existe des appareils de vision nocturnes pour espionner les rendez-vous plus «champêtres». Autrefois réservés à l'armée et aux services secrets, ces accessoires deviennent des objets presque courants… Grâce à eux et en pleine nuit, vous voyez presque comme en plein jour, et de loin… Ce sont, là encore, les Québécois qui proposent un catalogue complet: vision de nuit de type monoculaire ou binoculaire, miniaturisé ou non. Certains d'entre eux peuvent être équipés d'un appareil photo mais dans tous les cas, ces gadgets ne passent pas inaperçus, vos observateurs seront obligés de se cacher; par contre, il n'existe pas vraiment de moyen de les repérer, à vous de vous cacher à votre tour! Et puis sachez que même s'ils deviennent de plus en plus courants, ces appareils coûtent encore chers, n'importe qui ne peut pas investir de 5000 à 10.000F, quoique les prix baissent d'année en année!

Entre la France, le Québec et l'Espagne, l'internaute qui s'est découvert une vocation d'espion a donc fort à faire… De son fauteuil, confortablement installé derrière son PC, il peut faire ses courses, et se tenir au courant des progrès de la technologie. Audio, vidéo, vision nocturne… Rien ne manque! Au chapitre des trouvailles plus insolites, les espions peuvent également se fabriquer une fausse identité… Passeport, carte d'identité, cartes professionnelles, carte d'étudiant, le choix est impressionnant. Ce sont apparemment les Américains qui sont les clients les plus friands. Quelque peu paranoïaques, ils craignent que le fait d'être américain leur attire les foudres de tous les terroristes du monde. En cas de détournement d'avion, de prise d'otages, ils préfèrent avoir sur eux un faux passeport qui serait susceptible de leur sauver la vie. C'est en général de cette façon que les sites de faux papiers vantent leurs mérites. Les espions en herbe ne manqueront d'utiliser ces documents à d'autres fins… Il est toujours spectaculaire d'arriver sur un site et de se croire dans un véritable supermarché! Espionnage-store.com, par exemple, propose de nombreuses rubriques dédiées aux faux-papiers: diplômes, cartes professionnelles, passeports… Vous cliquez sur ce dont vous avez besoin et vous choisissez! Petit détail, c'est un site anglophone, n'y cherchez pas des documents français. Les diplômes, par exemple, pour 200F, vous devenez bachelier, diplômé de plongée sous-marine, agent du Mossad ou journaliste! Reste à voir la qualité! Pour 150F, vous pouvez obtenir la carte professionnelle de votre choix; agent de voyage, notaire, acteur, spécialistes en armes à feu… Mais que fait la police?

Devenir un citoyen du Honduras, pas de problème, envoyez environ 3000F pour un passeport standard et 3500F pour un passeport diplomatique. Tout simplement incroyable! D'autres pays se font un plaisir de vous vendre des passeports en Amérique latine: le Paraguay, le Nicaragua entre autres. De nombreux pays, dans le monde, proposent un passeport moyennant finances; ce sont, en général, des pays en voie de développement peu regardants sur l'identité du demandeur. Le pire, c'est que certains d'entre eux sont capables de vendre des faux-passeports de la nationalité de votre choix: américains, anglais, français… Gageons que les douaniers sont au courant et qu'ils ouvriront l'œil!

Cette expérience prouve que - d'un clic de souris -, vous pouvez devenir un parfait espion grâce au Web… Micros-espions, écoutes téléphoniques, minis-caméras… Tout l'arsenal est disponible, il suffit d'y mettre le prix. Heureusement, les moyens de contre-espionnage existent mais ils coûtent aussi chers (sinon plus!). Quoi qu'il en soit, il peut être intéressant de connaître les gadgets qui existent afin de mieux se protéger: un homme averti en vaut deux! Sachez tout de même que les agents secrets -les vrais!- ont toujours une longueur d'avance. Ils peuvent acheter du matériel dans le commerce, tel que celui dont nous avons parlé, mais il sera transformé et adapté à leurs besoins. Souvenez-vous du célèbre «Q» des James Bond, cet ingénieur à l'imagination fertile disposait d'un laboratoire extraordinaire. Pour s'en rendre compte, il suffit de se rendre sur le site de la CIA américaine. Un musée des gadgets «genre 007» est présenté au public… C'est passionnant à regarder et cela donne une idée de ce que les ingénieurs étaient capables de faire (**www.cia.gov**).

Par contre, ces accessoires datent des années… 60! **Il faudra attendre encore 40 ans pour savoir ce que les espions utilisent aujourd'hui, dommage!**

Interview

Incollable sur James Bond!

François-Xavier Busnel, 37 ans, est tombé dans la marmite des James Bond lorsqu'il avait 10 ans. Il a alors assisté à sa première projection et il a commencé à collectionner ce qui lui rappelait 007. Aujourd'hui il est incollable sur tout ce qui concerne James Bond et ses connaissances sont regroupées au sein de deux sites -jamesbond007.net et www.jamesbond collectibles.com- dont il est le webmaster.

Hacker News Magazine : *Pour vous, ce sont les James Bond qui ont inspiré les services d'espionnage en matière de gadgets ou le contraire?*

François-Xavier Busnel: «Les gadgets sont vraiment apparus au moment de la Seconde Guerre Mondiale et Ian Fleming s'est largement inspiré du travail effectué par les services secrets britanniques (où il travaillait pendant la guerre) dans ses romans.»

HNM : Quels sont les gadgets 007 les plus réussis?

A.K. : «Pour Bond, les montres jouent et ont joué un rôle important dans ses missions de même que l'équipement spécial de ses voitures. Hormis cela on peut citer en vrac, le détecteur de micros, le dentifrice explosif, le lance-fléchettes attaché au poignet, la mallette standard de la Section Q, le pince-doigts qui évite de se faire voler son arme, la carte de crédit qui ouvre les serrures…

HNM : *Si Ian Fleming était encore de ce monde, il ne manquerait pas de sujets pour des projets de gadgets: Internet, MP3, téléphones mobiles… Quels sont les technologies qu'il préférerait et qu'en ferait-il par exemple?*

F-X.B. : «Je pense que la toile aurait (pourrait car c'est maintenant un américain, Raymond Benson qui écrit les romans 007) pu être -pour Ian Fleming- un excellent terrain de jeux de même que la surveillance quasi continuelle des personnes par l'intermédiaire des portables et des cartes de crédit.»

HNM : James Bond ferait-il encore un bon espion en l'an 2001?

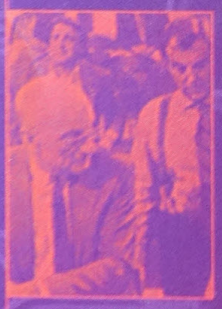
F.-X.B.: «A l'écran certainement, le box-office est là pour en témoigner, au sein du MI6 (NDLR: les services secrets britanniques) cela me paraît plus difficile, la discrétion est de mise et ce n'est pas le fort de l'agent 007.»

ChaosComputerClub

>>>Il existe en Europe, depuis les années 80, un groupe de hackers pas comme les autres. Ils sont allemands, ont fait les 400 coups mais sont restés dans le droit chemin. Ils sont membres de la même équipe, celle du C.C.C., le Chaos Computer Club...<<<

la communauté galactique

L'idée de ce groupe, Liberté d'expression et informatique sans maîtres. Le Chaos revendique d'ailleurs la liberté de l'information arguant qu'il est impératif que les gens puissent se faire une opinion par eux-mêmes. En 1984, ils lanceront leur manifeste : «Nous réclamons la reconnaissance d'un nouveau droit de l'homme, le droit de la communication libre, sans entrave, à travers le monde entier, entre tous les hommes et tous les êtres doués d'intelligence, sans exception. Les ordinateurs sont des instruments de jeu, de travail et de pensée. Mais il est surtout le plus important des nouveaux médias. Nous nous élevons contre la politique de panique et de crétinisation qui sévit en matière d'ordinateurs, de même que contre les mesures de censure de groupements industriels internationaux, des monopoles des postes et gouvernements». Pour faire passer son message, le C.C.C. usera des médias pour s'assurer que le public puisse véritablement se faire sa propre opinion sur le merveilleux monde qu'est l'informatique. Son fondateur, Wau Holland, explique ses agissements et celui de son groupe comme « Un acte de création, pratique et irrespectueux».



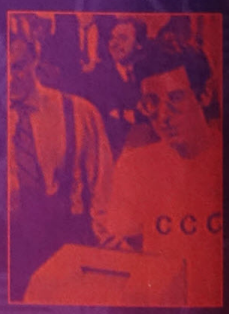
Le premier coup d'éclat du C.C.C. se réalisera en 1984, de mémoire de vieux briscard de la micro, un coup qui restera gravé dans toutes les mémoires. Les hackers du C.C.C. détourneront 135 000 marks via la Caisse d'épargne de Hambourg. «Informer le public» était l'unique but avoué à l'époque. En 1997, des membres du Chaos Computer Club démontreront, en direct à la télévision allemande, la défaillance d'un logiciel utilisant les ActivX de Microsoft. Ce logiciel était destiné aux agences bancaires. Il devait permettre les transactions d'argent d'un compte à un autre. Le Chaos Computer Club s'impose donc très vite comme le groupe représentatif de l'idéologie du hacking. «Ne rien détruire mais donner la réplique aux abus du corporatisme technologique.» Le problème est que le C.C.C. a souvent divulgué ses actes après que la presse en parle dans ses colonnes. Le C.C.C. jouait-il un double jeu dans les années 80 ?

> Hacker blanc et hacker rouge

Fin des années 80, le C.C.C. est devenu un groupe de référence fort d'une centaine d'adhérents et prêt de 400 sympathisants. Dans ce groupe, des ado, des ingénieurs, maîtrisant parfaitement l'informatique et donc cible parfaite pour des services de renseignements étrangers, comme le KGB, qui ne s'y trompera pas.

Des membres du C.C.C. pirateront de grandes sociétés, telles que Thomson, le CERN ou encore le CRAY de polytechnique. Le piratage de ce super calculateur était considéré, à l'époque, comme impossible. Le KGB apparaît dans l'affaire du piratage du VAX de Philips France en 1986 à Fontenay-sous-bois. A cette époque Philips travaille avec les militaires sur un projet proche des missiles Exocet. Des informations sont volées et revendues à l'URSS. L'un des pirates, membre du C.C.C., sera d'ailleurs retrouvé par la police allemande, mort dans un mystérieux incendie à Hanovre.

Le C.C.C. connaîtra d'autres incidents et un autre décès, tout aussi mystérieux. Ce nouveau mort se nomme TRON, un génial concepteur dans sa spécialisation, la cryptographie. Il sera retrouvé mort, dans le parc de Neukölln à Berlin. Pendu avec sa ceinture, le problème est que ses pieds touchaient le sol. Le C.C.C. communiquera son avis sur le sujet : «Les sources de la police laissent à croire qu'il s'agirait d'un suicide. Nous ne partageons pas du tout cette opinion. Tron fut l'une des plus brillantes têtes de file des hackers en Europe. Il présenta les possibilités d'élaboration de cartes contrefaites pour les téléphones publics. Il développa et conclut la première de ces "miracle cards". Poussé par l'envie de rechercher et d'explorer toutes les possibilités techniques, il frôla les limites des lois et fut condamné avec sursis. Après cette expérience, il ressentit le besoin de tirer un trait et contacta le Chaos Computer Club. Il utilisa ensuite son énergie créative et son potentiel sur des projets qui

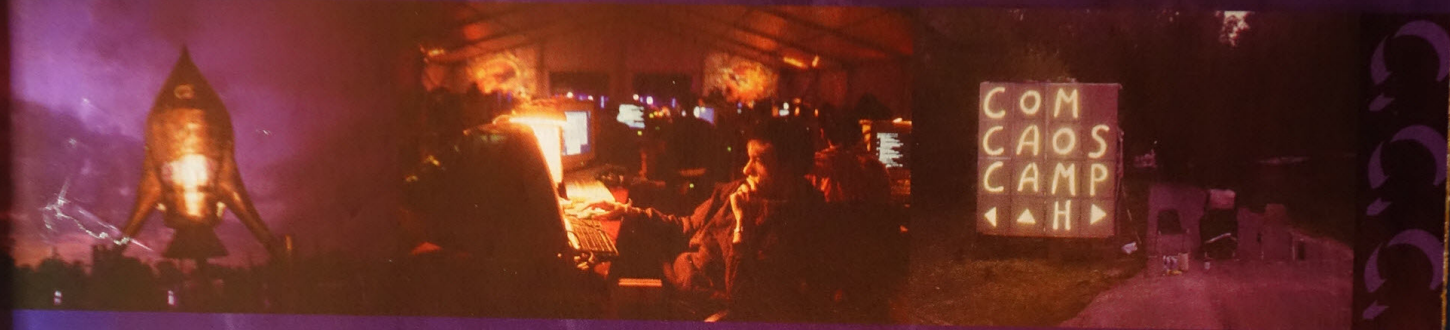


Interview de J.B. Condat, C.C.C.F. avant son arrestation
http://the.wiretapped.net/security/info/textfiles/chaos-digest/chaos-digest-73.txt

Interview de J.B. Condat, C.C.C.F. après son arrestation
http://www.magic.be/InterieurNuit/SiteMars/Condat.html

Le site du C.C.C.
http://www.ccc.de/

L'interview d'Andy Müller-Maghun
http://www.zataz.com/portraits/



ne lui poseraient plus de problèmes avec la loi. Dans sa récente thèse, il écrivit sur l'utilisation de systèmes modernes de cryptage dans les télécommunications. Le montage qu'il développa et présenta: un Brouilleur à faible coût utilisant des méthodes de cryptage pour sécuriser les conversations téléphoniques sur les lignes ISDN, devint un standard due à sa simplicité et sa taille compacte. TRON fut aussi un de ceux qui présenta le moyen de cloner les smart cards GSM en Allemagne. Son grand savoir et sa créativité jouèrent un grand rôle dans le succès de son projet. TRON a toujours eu un caractère direct et une personnalité très ouverte et n'a jamais eu de problèmes. Nous ne voyons aucune raison pour lui de s'être suicidé et nous espérons avoir plus d'information par l'enquête de la police.» Alors que le C.C.C. est devenu, en 1986, une organisation légale, la police de Hambourg, à la demande d'un juge français, perquisitionne, en 1987, les locaux du C.C.C., suite au piratage de Philips. Bilan, la justice va découvrir que des membres du C.C.C. ont piraté le C.E.A. français, le C.N.R.S., l'Observatoire de Paris, la N.A.S.A.,... En 1989, la B.F.V., équivalent de notre service français, la D.S.T. arrête une dizaine de membres du C.C.C. qui ont eu la fâcheuse habitude de pirater des sites militaires américains et des centres de recherches de l'aérospatiale et nucléaire. Ils travaillaient pour le KGB, depuis 1985, en échange d'argent et de drogue. La D.S.T. découvrira que le piratage de Thomson ne servait en fait que de passerelle entre les pirates allemands et les services de renseignements russes.

> Le C.C.C. France, piége à pirates

Fin des années 80, la France commence sérieusement à s'inquiéter de ces intrusions. Via son service de contre espionnage, la Direction de la Surveillance du Territoire, l'Hexagone va mettre en place un club identique au C.C.C. de Hambourg. Il sera créé en 1989 et sera judicieusement nommé le C.C.C. France. A sa tête, Jean Bernard Condat, un jeune informaticien, comme porte-parole et J.L.D. son officier de liaison.

Le but de ce «club» consistait à regrouper des pirates sous la même bannière, tracer leurs savoir-faire et remonter les piratages et leurs acteurs. Il ne faudra pas bien longtemps à la D.S.T. pour organiser ce qui est encore appelé aujourd'hui «LA grande rafle» avec pas moins d'une cinquantaine de jeunes pirates arrêtés.

Le site ZATAZ.COM a interrogé un responsable de la D.S.T. à ce sujet, voilà ce que répond ce policier à la question, la D.S.T. avait-t-elle vraiment infiltré ce club ? : «A partir du moment où on s'intéresse à ce qui se passe dans ces milieux-là, on diligente des enquêtes tant en France que sur le plan international dans la mesure ou l'Internet abolit les frontières. Nous avions une enquête en cours sur des affaires d'intrusions sur notre territoire qui nous a amené à identifier des auteurs qui se situaient en Allemagne. L'enquête au sujet de certains membres notamment du Chaos Computer Club allemand, a montré qu'ils ont voulu vendre des informations aux services secrets soviétiques (K.G.B.) ».

Voici un extrait d'une interview de monsieur Condat trouvée sur le web. «Au C.C.C.F. nous ne sommes que 72, on ne peut pas être plus dans notre groupe... On les prend à la sortie de Polytechnique, généralement ils sont membres de la Mensa, sains de corps et d'esprit, ayant de quoi vivre largement au-dessus de leurs moyens, et moi je suis la carotte. Moi, je suis secrétaire général, je suis là pour parler et émettre, mais je suis le plus con de tous. En informatique, je ne sais rien. Je ne suis pas la cheville ouvrière, mais la reine (ou le roi) visible de l'essaim (...) Tous les services du monde ont essayé de nous approcher, sauf les services français. Ils ne vous approchent pas. Ils vous piétinent, et après ils vous demandent l'autorisation.» Le C.C.C.F. n'existe plus depuis 1991 et Jean Bernard Condat est une marque déposée.

> Le C.C.C. aujourd'hui

En ce début de siècle, le C.C.C. de Hambourg est devenu une association comme les autres, connue et reconnue, avec ses petites fêtes, ses conférences et ses coups d'éclats. Le dernier en date, la remise du prix Big Brother, lors du CeBIT 2001, à la société Siemens. Un prix satirique pour le logiciel "Smart-Filter" un filtre qui "Censure Internet et la communication." L'autre grand coup du C.C.C. est l'élection d'Andy Müller-Maghun, représentant européen auprès de l'Icann, l'organisme chargée de la gestion des noms de domaine, mais aussi et surtout, le porte-parole du Chaos. Il sera élu le 10 octobre 2000 avec 5 948 voix et représente du coup l'Europe au sein du Conseil d'Administration de l'Icann. "Je ne cache pas que j'ai été surpris d'être en tête dans cette élection. Comme porte-parole du Chaos Computer Club je semble être bien connu en tant que personne qui représente les intérêts de la communauté des internautes. Liberté de parole, intimité et maintenir l'Internet comme un espace public sans que cela ne devienne la chasse gardée des compagnies ou des gouvernements. Je pense que les gens s'attendent à ce que j'introduise nos positions de liberté dans les discussions au sujet de l'architecture du Web, de sorte que de futures politiques et règles ne soient pas faites uniquement par les industriels." Expliquera-t-il. L'idée de communauté galactique est toujours aussi présente.

LOFT STORY

je t'aime, moi non plus

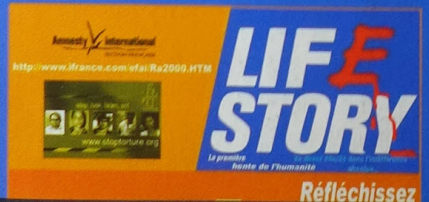
>>>Pendant plusieurs semaines M6 a tenu le haut du pavé avec son émission Loft Story. <<<

Une première place qui n'a pas plus à tout le monde. Le réseau des réseaux a été le moyen, pour ceux qui trouvaient cette émission "trop indiscrète" de s'exprimer, quitte à pirater le site web officiel et l'organisation de ce Reality Show.

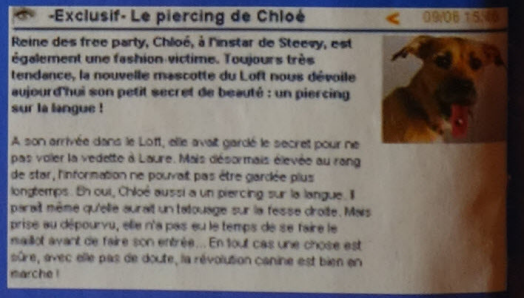
> De la rumeur à l'acte

Vendredi 27 avril, la rumeur fait entendre qu'un pirate aurait accès au serveur web de l'émission Loft Story. Une information qui n'avait pas vraiment étonné vu le nom de l'hebergeur du site web, la société Atos. Un fournisseur d'espace connu pour ne pas vraiment être à cheval sur la sécurité informatique. Quelques heures après l'alerte donnée sur l'Internet Relay Chat (l'IRC), le site web tombait sous les coups d'un vengeur masqué, nommé M. Tordu. Il signera son acte d'un message clair et sans équivoque : "La première fiction de merde".

On vous passe les insultes à l'encontre de l'animateur de l'émission, Benjamin Castaldi. L'auteur de ce piratage sera d'ailleurs interviewé dans les colonnes de Transfert. Il justifiera son acte ainsi : "Parce que s'il y a un truc qui me révolte, c'est bien l'abrutissement de la foule par les mass media. Surtout que tout ça est en accès libre !". Il y aura cinq autres piratages de ce site. Le plus marquant par son message, sera celui d'un "hacker" sans nom (Ndlr : il y a fort à parier que M. Tordu y est pour quelques chose) qui placera, en lieu et place du logo de LoftStory, un article sur le dernier rapport d'Amnistie International lié aux tortures dans le monde. En milieu de page, une image titrant «Life Story».



Les trois derniers piratages sont plutôt bizarres. Au lieu d'une modification de la page index, ce sont les pages news qui ont été touchées. On a pu y lire les interviews des amis de Chloé, la chienne participant à l'émission. Un jour, le chien Gaston parlant de sa meilleure amie, un autre jour, Chloé parlant de son piercing à la langue, ... Vrai piratage ou coup de « hacking-marketing » du webmaster ? Il est vrai que faire venir les internautes sur un faux piratage, obligeant ainsi les fans à cliquer sur plusieurs pages, donc plusieurs pubs, devait être tentant. Les visiteurs se faisaient-ils de plus en plus rares ? Le « hack-marketing » ne date pas d'hier, MTV avait lancé l'idée, en septembre 1998, en faisant croire à un piratage de son site internet. Un faux piratage pour une vraie promo.

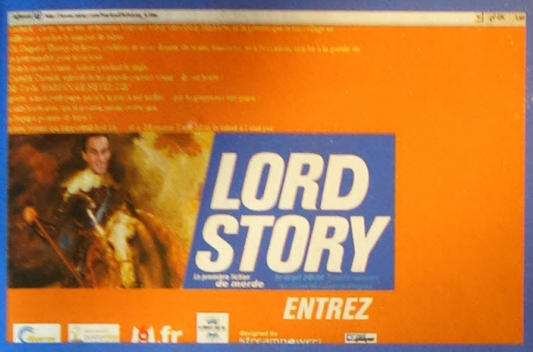

-Exclusif- Le piercing de Chloé

Reine des free party, Chloé, à l'instar de Steevy, est également une fashion victime. Toujours très tendance, la nouvelle mascotte du Loft nous dévoile aujourd'hui son petit secret de beauté : un piercing sur la langue !

A son arrivée dans le Loft, elle avait gardé le secret pour ne pas voler la vedette à Laure. Mais désormais élevée au rang de star, l'information ne pouvait pas être gardée plus longtemps. Eh oui, Chloé aussi a un piercing sur la langue. Il paraît même qu'elle aurait un tatouage sur la fesse droite. Mais prise au dépourvu, elle n'a pas eu le temps de se faire le maillot avant de faire son entrée... En tout cas une chose est sûre, avec elle pas de doute, la révolution canine est bien en marche !

> Petite visite de courtoisie

Plusieurs sites « anti » Loft-story lanceront une action symbolique « Sauvons les lofteurs ». L'un des coups les plus marquants, surtout pour son auteur, aura été l'intrusion dans le Loft par un jeune parisien, nommé Neurone. Il discutera quelques secondes avec les lofteurs, lui dans le jardin, les participants dans le salon. Ce visiteur d'un soir connaîtra aussi les joies des vigiles de la production.



L'interview de M. Tordu
http://fr.news.yahoo.com/010430/166/18w6x.html

LOFT STORY

> Logiciels d'amateurs

Pendant la durée de cette émission une vraie course poursuite a été lancée par M6 pour traquer les diffusions pirates de ses webcams. M6 ne souhaitait qu'une chose, que les mateurs passent uniquement par son site. La publicité était, bien sûr, le premier objectif. L'autre objectif était de s'assurer que les internautes verraient ce que M6 avaient décidé de montrer.

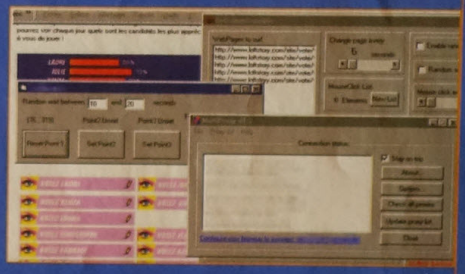
L'affaire des vidéos "pornos" de deux lofteurs dans la piscine puis dans la chambre avaient mis le feu au poudre. M6 ayant même communiqué sur le fait que des pirates avait réussi à voler ces scènes sur leurs serveurs. Une affaire qui fait encore rire aujourd'hui la scène Vidcaps/scans. Une scène d'initiés qui est dédiée uniquement à tout ce qui touche aux captures vidéos et photos et diffusées ensuite sur le réseau. L'un des membres de cette scène, GaKaTan, est l'un des premiers à avoir eu dans les mains cette vidéo. « Une capture réalisée par un contact via... TPS » nous confiera-t-il. A la question, est ce que ces vidéos ont été volées dans les serveurs de l'émission ? Sa réponse sera sans équivoque : « Ridicule ! Les seuls pirates du Loft ont été ceux qui ont modifié plusieurs fois la page d'accueil. Tout ceci est une excuse pour se dé-responsabiliser envers les lofteurs et leurs familles qui pourraient porter plainte. Les premières vidéos du Loft qui ont circulé (Salle de bains, piscine...) viennent de TPS. Les premiers jours de l'émission, le réalisateur et les caméramans appliquait le "0% censure". Et puis après cette affaire, plus rien. Ce qui explique pourquoi plus de nouvelles vidéos "X" circulent sur le net. » Un coup de publicité pour par cher avec en plus une contre attaque de la petite chaîne qui monte. Des dizaines de courriers du service juridique de M6 obligeant les sites non-officiels diffusant ces vidéos de les effacer ou de fermer. Beaucoup, par crainte du gendarme, vont obtempérer. D'autres, surtout des sites pornos basés hors de la France, continuent de diffuser Jean-édouard apprenant la natation à Loana.

D'autres internautes, amateurs et fans de cette émission, réaliseront une dizaine de logiciels permettant de trouver en temps réel les flux vidéos de M6. Des logiciels d'une efficacité redoutable car certains permettaient même d'afficher deux flux vidéo en même temps. Un gadget qui a permis de regarder certaines scènes jamais diffusées sur TPS. Un exemple : Le survol de la prison dorée par un hélicoptère obligeant le staff technique de l'émission à enfermer les lofteurs dans leur chambre. M6 tentera aussi de bloquer ses fans un peu trop curieux, avec des tentatives de blocage des logiciels, sans grand succès. Ils iront jusqu'à mettre en place un IP différent par internaute. Pas plus de succès car les logiciels « pirates » seront mis à jour dans la foulée, quelques heures plus tard, pour contrer cette « protection ».

La chaîne trouvera quand même le moyen de qualifier les sites officieux de "sites pirates" et "de hackers" les internautes qui trouvaient les url des caméras. Il est vrai que la qualité proposée par ces logiciels "pirates" était bien supérieure à celle proposée par M6. Ils permettaient aussi de ne pas se farcir dix publicités avant que le site… fasse planter votre ordinateur.

> Trucage des votes !

Un groupe d'internautes a voulu tester les votes de l'émission, juste comme ça, pour voir. L'un des investigateurs se nommait TheTeacher. Son truc à lui a été de tester le système de votes du site web. Un système qui au début de l'émission permettait de "mettre à la porte" certains participants du loft. La mise en place de ce trucage était simple. Trois logiciels, dont multi-proxy. Le premier logiciel modifiait les IP à chaque affichage de la page des votes ; le second programme lançait



la page web des votes toutes les 10 secondes ; le troisième et dernier soft cliquait sur les liens qui avaient été définis. (Ndlr : Cette méthode est utilisée par des webmasters peu scrupuleux, souhaitant truquer le nombre de click sur leurs banderoles publicitaire affichait sur leurs sites web.)

Est-ce que le trucage à fonctionné ? Personne ne le saura vraiment. Chose étrange, quelques jours après la découverte de la mise en place de ce trucage, le site LoftStory ne proposait plus de voter pour éliminer mais pour garder les lofteurs. La technique de trucage n'était plus utile... du moins sur le site car il restait les votes via GSM. Ici aussi le trucage a été tenté. Le fonctionnement était toujours aussi simple. Des dizaines de sites web proposent d'envoyer des SMS gratuitement. Des internautes ont donc mis en place plusieurs logiciels permettant de garder un anonymat certains et de permettre le voter via ces pages internet.

Ici aussi, on ne connaîtra jamais les résultats de cette tentative de trucage. Une chose est certaine, sur un week-end, pas moins de 20 000 SMS ont été envoyées... sans aucun effet sur les statistiques des lofteurs ciblés pour cette expérience, soit Loana et ... Christophe !

Les attaques magnétiques sont-elles désormais à la portée de n'importe quel hacker?

>>> Déjà en 1996 aux USA, le sénateur Nunn avait mis en garde ses concitoyens contre la menace d'un "Pearl Harbor électronique". Une telle attaque, exécutée par un groupe terroriste contre des réseaux de communication, paralyserait non seulement ses communications mais aussi le système financier et les transports.

Depuis longtemps les militaires protègent leurs systèmes électroniques des radiations électromagnétiques qui seraient produites lors d'une explosion nucléaire. Sans contre-mesures adéquates, il est en effet possible de détruire les systèmes électroniques d'un pays en faisant exploser une bombe atomique à haute altitude. Ce type de bombe n'est heureusement pas à la portée du premier venu. Mais la technologie évoluant, il est désormais à la portée d'un hacker de construire à moindre frais un appareil pouvant détériorer, à distance, des ordinateurs. C'est ce que vient de prouver un scientifique aux Etats-Unis. Votre ordinateur utilise au sens large un courant d'électrons. Ce "vecteur informatique" circule au sein de circuits électroniques, file le long de câbles et en général finit sa course sur un support dit «électromagnétique».

Pour rappel, le flux électromagnétique se présente sous la forme d'une onde et d'une particule que l'on nomme un photon. Le spectre électromagnétique s'étend depuis les très grandes longueurs d'onde radio (10 km), jusqu'aux rayons gamma dont la longueur d'onde associée est très courte. A ce niveau et en matière de sécurité informatique trois problèmes peuvent se présenter.

Longueur d'onde la distance de déplacement de l'onde pendant une seconde qui est inversement proportionnelle à la fréquence (plus celle-ci est élevée, plus la longueur d'onde est courte).

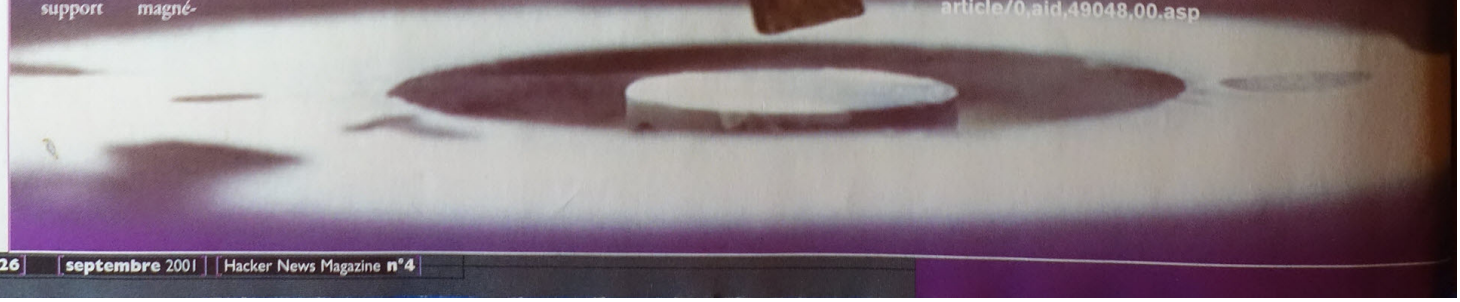
Le premier problème est celui de la longévité des informations enregistrées sur support magnétique. En raison de l'action du champ magnétique terrestre, les informations enregistrées sur disquette, cartouches zip ou autres supports magnétiques s'effacent avec le temps. L'avantage d'un support magnétique est son faible coût. L'inconvénient est sa courte durée de vie qui entraîne l'altération du signal au bout de 15 ans (selon la qualité de l'enregistrement initial et des précautions prises lors du stockage). Il est donc très facile de détériorer un support magnétique car un simple aimant suffit. Ouvrons d'ailleurs une parenthèse pour signaler que si vous avez enregistré votre cérémonie de mariage sur une cassette vidéo, vous devrez un jour la numériser pour ensuite la graver sur cd-rom (Divx) ou DVD. Sinon, 20 ans plus tard, vous prenez le risque de ne plus pouvoir la visionner à nouveau pour en faire profiter vos enfants ! La durée de vie des CD inscriptibles, dans des conditions normales de stockage, au sein d'un environnement de bureau ou domestique, est supérieure à 100 ans.

La circulation du flux électromagnétique au sein de votre ordinateur présente une autre particularité qui est celle du rayonnement. Un conducteur parcourut par un courant électrique est émetteur d'un champ électro-magnétique qui peut être intercepté par une tierce personne. Heureusement, la faible puissance mise en jeu limite très fortement la portée d'une telle écoute clandestine. Sans compter la nécessité de se procurer un équipement d'interception très onéreux. Autrement dit, votre écran d'ordinateur émet des radiations et il est possible avec l'équipement adéquat de reconstituer le contenu de celui-ci à distance. Cette technique a déjà été employée par le FBI avec un équipement du nom de «TEMPEST monitoring».

Outre ce problème de persistance et d'émission, une autre caractéristique des ondes électromagnétiques est la nature invisible du phénomène (exceptée la plage des 4000 (violet) à 7000 (rouge) angströms). Même si cette caractéristique est bien connue elle explique la faible sensibilisation du public face à une attaque du type électromagnétique. Récemment aux Etats-Unis un scientifique a prouvé qu'une attaque terroriste de type magnétique était à la portée de (presque) n'importe qui. En effet, il a élaboré cette machine infernale à partir de pièces détachées qu'il a pu trouver dans une grande surface spécialisée en électronique. Cet équipement occupe l'espace d'une fourgonnette et est par conséquent très mobile. Une fois celle-ci mise en marche, elle affecte directement les ordinateurs et autres appareils électroniques qui n'ont pas été spécialement protégés contre cette agression. Soit le blocage s'en suit, soit l'ordinateur tombe purement et simplement en panne. Le budget nécessaire à sa construction est de l'ordre de 10.000 Euros.

Si le particulier n'a pas vraiment à s'inquiéter, les industriels qui stockent ou utilisent des données sensibles doivent se rendre compte de cette possibilité. Des moyens existent pour s'en protéger (plus ou moins efficacement) mais encore faut-il prendre conscience du danger.

Pour en savoir plus:
http://www.pcworld.com/news/article/0,aid,49048,00.asp



ECHELON

>>> Souriez, vos e-mails sont lus… Et si ce n'était que ça… **Non seulement, dorénavant, vos e-mails peuvent être lus par des tiers, d'où qu'ils soient envoyés dans le monde, mais il en va de même pour les conversations téléphoniques, filaires ou cellulaires… Inquiétant ?…** Non, simplement réaliste ! Tout le monde s'en doutait depuis longtemps, le mythe du célèbre Big Brother planait au dessus de nos PC et de nos téléphones ; ça y est ! La NSA l'a fait ! Mais qui est-elle donc, cette fameuse NSA ?

Une surveillance à l'Échelon planétaire

La National Security Agency (Agence Nationale de Sécurité) porte très mal son nom… En effet, on pourrait croire que cette vénérable institution (son existence remonte quand même à 1941 !) a pour vocation de protéger un pays en particulier… Et bien non ! A l'origine, le projet de la NSA a démarré en 1941 en Grande-Bretagne, née de la coopération des Anglais et des Américains (l'agence a été officieusement créée en 1952, officiellement en 1957 !). Ces derniers, considérablement refroidis par l'attaque japonaise de Pearl Harbor, décident alors de constituer une agence capable d'intercepter les

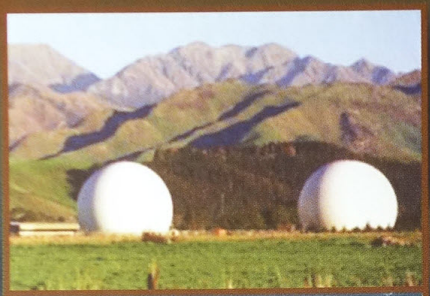
ECHELON

1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954

Naissance du Pacte UKUSA de coopération entre les Etats-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande.

Les grandes dates de la NSA

communications ennemies ; à l'époque les Japonais et les Allemands. Le coup d'envoi est donné, l'avenir de la NSA ne cessera plus de se présenter sous les meilleurs cieux qui soient. Un premier centre d'écoute est donc créé en Grande-Bretagne, à Bletchley Park et des « petits frères » ne tardent pas à le rejoindre ; en 1946, c'est au tour de Hong-Kong : une fructueuse collaboration internationale est en train de naître. La NSA prend déjà l'apparence qu'elle revêt aujourd'hui... L'objectif de l'agence est clairement défini, il s'agit d'une coopération en matière de renseignement électronique entre plusieurs pays alliés. Les acteurs de cette coopération se positionnent stratégiquement : les USA, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande. De quoi « couvrir » le monde entier... Nous sommes en 1948, le pacte UK-USA est signé et l'ennemi Numéro Un n'est autre que l'URSS.



La station de Waihopai en Nouvelle-Zélande.

> La maîtrise des télécommunications passe par l'espace

Les choses ont bien changé depuis... Les Russes ne font pas encore partie des programmes de la NSA mais cela pourrait bien ne pas tarder ! Cependant, il y a bien une chose qui n'a pas changé en 50 ans : on retrouve toujours le même leitmotiv et les mêmes alliés. D'ailleurs, il est surprenant de constater la persévérance avec laquelle les membres de la NSA ont su mener à bien ce projet. En 1941, les interceptions ne concernaient que les communications militaires. C'était le projet ULTRA... Aujourd'hui, il n'y a quasiment plus de restrictions, c'est le projet ECHELON. Un programme qui prend des dimensions inquiétantes, comme nous allons le voir. Mais auparavant, pour comprendre la démarche de cette surveillance, il faut savoir qu'entre ces deux projets, de nombreuses étapes ont jalonné l'histoire de la NSA. C'est donc en 1947 qu'un pacte est signé entre les deux principaux protagonistes de la NSA, les Etats-Unis et la Grande-Bretagne. Un an après, le Canada, l'Australie et la Nouvelle-Zélande complètent le pacte qui a pour objectif l'espionnage des télécommunications. Pour y parvenir, les pays membres décident que leurs services de renseignement pourront collaborer étroitement, et surtout, ils mettent en œuvre un ambitieux programme technologique selon deux grands axes. Le premier concerne les opérations SIGINT (Signal Intelligence), autrement dit l'espionnage électromagnétique dont les cibles sont : les liaisons radios, les émissions radars, les télécommunications… Le second axe est plus « confidentiel » car il s'agit de concevoir des systèmes de codage et de cryptage à des fins gouvernementales et militaires.

Petit à petit, le réseau grandit à travers le monde et ses moyens augmentent. En 1960-61, la NRO (National Reconnaissance Office) fait son apparition aux Etats-Unis. C'est une agence qui est chargée de fabriquer des satellites-espions. L'Oncle Sam voit déjà grand, il comprend que la maîtrise des télécommunications passe par la maîtrise de l'espace. Cette donnée peut éclairer une polémique qui gonfle à l'époque aux Etats-Unis : pourquoi dépenser autant d'argent dans une course sans fin à la conquête de l'espace contre l'URSS ? La question n'était sans doute pas de savoir qui marcherait le premier sur la Lune, mais plutôt de prendre de l'avance dans un domaine qui verrait des applications déterminantes !

> Menwith-Hill : la plus grande antenne satellitaire

Autre date-clé, l'année 1966 voit la prise de contrôle de la base de Menwith Hill (nord de l'Angleterre) par la NSA. Jusque là, cette base appartenait à l'armée américaine mais son rôle est redéfini, et pas à moitié car elle deviendra la plus grande station d'interception du monde ! Les années 70 seront jalonnées par les constructions de nouvelles stations : celle de Yakima aux Etats-Unis en 1970, son antenne est orientée vers le Pacifique et elle est prête à recevoir les informations de satellites INTELSAT. En 1972, c'est au tour de Morwenstow en Angleterre où pas moins de trente antennes satellitaires sont tournées vers l'Atlantique et l'océan Indien. Toujours à Menwith Hill, en Angleterre, l'ancêtre des stations est dotée de la première grande antenne satellitaire. En 1980, retour aux Etats-Unis où la station de Sugar Grove s'adapte à la deuxième génération de satellites INTELSAT. La même année, une autre station est construite à Hong-Kong.

Ces technologies peuvent paraître banales de nos jours, mais dans les années 40-60, ce sont des procédés qui en étaient à leurs balbutiements et les citoyens ignoraient totalement ce qui se passait. D'ailleurs, l'existence même de la NSA était officieuse. Il faudra attendre 1957 pour que le gouvernement américain la reconnaisse officiellement ! Il ne faut pas oublier que nous étions au cœur de la Guerre Froide ; les joutes entre les Etats-Unis et l'URSS ne cessaient jamais, par espions interposés. Ainsi, lorsque le mur de Berlin est tombé, la NSA s'est retrouvée sans objectif défini. Les pays de l'Est étant en déconfiture, le communisme agonisant, à quoi pourrait bien servir ce gigantesque réseau d'écoute ? D'après un ancien responsable des services secrets français, l'Amiral Pierre Lacoste : « la conquête des marchés mondiaux est désormais la nouvelle frontière des Américains ». Il paraît notamment, que la NSA aurait joué un rôle important lors des négociations du GATT sur le commerce mondial. Faut-il y voir un tournant et la naissance d'ECHELON ? Peut être… La date de naissance d'ECHELON est inconnue à ce jour, mais qu'importe le nom de ce programme. Qu'il s'appelle

Menwith Hill, en Grande-Bretagne, est devenue la plus grande station d'écoute de la planète. Elle suscite, sur place, de virulentes réactions de la part de ses opposants qui ont même créé un site Web (**www.gn.apc.org/cndyorks/mhs/index.htm**).

Photo : Aurel Duta

Les grandes dates de la NSA

1956 **1957** 1958 1959 **1960** 1961 1962 1963 1964 1965 **1966** 1967 1968 1969 **1970**

Naissance officielle de la National Security Agency.

La base de Menwith Hill en Grande-Bretagne -une des premières stations d'écoute-, est contrôlée par la NSA.

Apparition de la première génération de satellites INTELSAT et création de la station de Yakima aux USA.

ECHELON

ULTRA ou ECHELON, la finalité du projet n'a jamais dévié d'un millimètre : pouvoir intercepter n'importe quelle communication, dans n'importe quel point du globe. Le premier réseau global à grande échelle est créé en 1981, il porte le nom de Wan. Le principe n'est pas très éloigné de celui du réseau Internet qui sévit déjà à l'époque. Les stations de surveillance et les centres de traitement sont reliés entre eux grâce à des câbles transocéaniques et à des liaisons spatiales. Il faut rappeler à ce sujet que le réseau Internet, inventé par des militaires américains, consistait à relier plusieurs bases militaires par l'intermédiaire du réseau téléphonique.

> Un journaliste parle du projet ECHELON en 1988

Il faudra attendre 1988 pour commencer à entendre parler du projet ECHELON, grâce à un journaliste, Duncan Campbell, qui publie un article dans l'hebdomadaire britannique « News Statesman ». Deux ans plus tard, les premières affaires d'interception font parler d'elles. En effet, en 1990, la NSA a écouté les communications entre le fabricant japonais NEC et l'Indonésie, qui voulait s'équiper en satellites. Les deux parties auraient pu s'en douter car en 1988, le ministre de la Défense néo-Zélandais avait révélé que deux nouvelles bases étaient en construction. L'objectif de ces stations n'était pas militaire, il ne faisait qu'anticiper la venue de futurs satellites provenant de l'Inde ou de l'Indonésie.

Cet épisode confirme ce que tout le monde pensait. Le prochain conflit ne sera pas la Troisième Guerre Mondiale, ce sera une bataille économique. Grâce à cette interception, George Bush, intervient à temps dans la négociation entre le Japon et l'Indonésie. Les Américains partageront le gâteau avec NEC et ils obtiendront un contrat de 200 millions de dollars par l'intermédiaire de la société ATT. C'est dire que les enjeux et les applications d'ECHELON sont énormes et cela ne fait que commencer. Du coup, de plus en plus de candidats sont intéressés par ce réseau miracle et depuis le pacte UK-USA, plusieurs pays se sont ajoutés à la liste initiale. A l'origine, le traité ne regroupait, en plus des Etats-Unis, que des pays membres du Commonwealth : la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande. Des participants tiers ont ensuite fait leur apparition à l'occasion d'un pacte secret : le Danemark, l'Allemagne et la Turquie. Enfin, la liste des pays alliés s'est encore agrandie avec la Corée du Sud, le Japon, la Suisse et Taiwan. Certaines de ces alliances sont éminemment stratégiques puisqu'il pouvait exister des zones d'ombre dans la couverture de la NSA… On peut naturellement parler de l'Europe. Les bases anglaises pouvaient se révéler insuffisantes à une époque, et la station de Bad Aibling a certainement joué un rôle déterminant, c'est la seconde installation la plus importante en Europe, après Menwith Hill. Ces questions n'ont apparemment plus cours… Bad Abling devrait fermer ses portes en 2002, les bases terrestres n'auraient plus de raisons d'être avec les performances des satellites-espions.

Le site officiel de la NSA (**www.nsa.gouv**) n'est qu'une vitrine très institutionnelle et tout à fait terne ; on y trouve aucune information digne d'intérêt sur ECHELON, évidemment !

> De « Grandes oreilles » réparties sur tous les continents

Bases terrestres, satellites-espions, mais au fait, ECHELON ? Comment ça marche ? D'après les informations indiscrètes qui ont pu filtrer à droite et à gauche, ECHELON marche bien. Peut-être même trop bien… C'est certainement pour cette raison que ce réseau d'écoute fait de plus en plus parler de lui. Dans les années 60-70, le grand public pouvait faire semblant de ne pas être inquiet car il pouvait croire que la NSA se limitait à intercepter les émissions radios, grâce à ses « grandes oreilles ». Aujourd'hui, les technologies mises en œuvre par la NSA dépassent largement ce champ de compétence. Les antennes continuent évidemment à servir, mais d'autres moyens sont venus les compléter : les satellites, l'écoute des câbles de raccordement, les ordinateurs… Les antennes -ces « grandes oreilles » réparties sur l'ensemble des continents-, sont la base technologique du réseau et il en existe différents types. Les antennes Wullenweber verticales sont disposées par rangées formant un cercle de grand diamètre ; elles sont prévues pour déterminer l'orientation des signaux hertziens. Les antennes de réception multidirectionnelles servent à intercepter des signaux hertziens non dirigés.

Enfin, celles qui sont de plus en plus répandues, les antennes paraboliques, sont utilisées pour capter les signaux satellitaires. Il semblerait que les « paraboles » jouent un rôle de plus en plus important en raison de leur champ d'action. Elles sont capables de recevoir des communications militaires, de capter les informations des satellites-espions (photos, radars….), d'intercepter les communications militaires et civiles. Ce cumul de fonctions les rend très performantes, sans compter que l'avenir des satellites paraît sans limites. De plus, les antennes paraboliques peuvent être installées à terre mais il est également possible d'en équiper des navires qui sont ainsi en mesure de se positionner à bon escient ; la NSA ne s'en prive pas grâce aux navires militaires. Ces antennes, quelles qu'elles soient, forment un réseau à travers plusieurs dizaines de bases dans le monde. Pour compléter ce réseau, plusieurs satellites sont au service de la NSA (Mercury, Mentor, Trompet).

> Plus de 20.000 employés travailleraient au Q-G de la NSA

Ces capteurs en orbite sont capables d'intercepter toutes les communications radio-électriques. Et c'est ce point qui est inquiétant… Cela signifie que tout appareil qui dégage des ondes est une source d'informations. Un poste de radio ou une télévision, bien sûr, mais surtout un téléphone portable, un four à micro-ondes… Les ingénieurs de la NSA tirent parti de tout

ECHELON

1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985

La première antenne satellitaire est mise en œuvre à Menwith Hill (Grande-Bretagne).

Apparition de la deuxième génération de satellites INTELSAT et créations des stations de Sugar Grove (Etats-Unis) et Hong-Kong.

le premier réseau global à grande échelle de surveillance des télécommunications (Wan) est constitué.

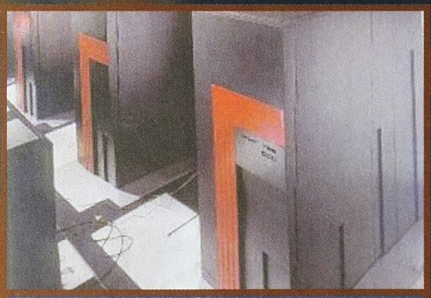
Les grandes dates de la NSA

ce qui peut leur servir. Même les câbles sous-marins qui relient les centraux téléphoniques seraient surveillés grâce à des robots qui installent des bretelles d'écoutes. Avec l'avènement des câbles à fibres optiques, ils ont dû faire face à un nouveau challenge et ils auraient trouvé un moyen de transformer l'impulsion optique en impulsion électrique afin de l'intercepter !Il faut dire que la NSA n'est pas exactement une agence d'apprentis bricoleurs et elle bénéficie de plus de 50 ans d'expérience au service du contre-espionnage… Le quartier général de l'agence, qui se trouve à Fort Meade aux Etats-Unis, abriterait quelque 20.000 employés. Il y a de nombreux techniciens - ingénieurs, analystes, physiciens, mathématiciens, informaticiens -, et des spécialistes de toutes sortes : officiers de sécurité, experts en flux de données…Il serait intéressant de connaître le budget alloué à la NSA. Nul doute que les analystes utilisent les ordinateurs les plus puissants qui soient car ce sont aujourd'hui les organes-clés de l'agence. En effet, les ingénieurs ont beau bénéficier de toutes les interceptions possibles, aux quatre coins de la planète, ils ne peuvent humainement pas trier ces millions, ces milliards d'informations.

Imaginez un instant, chaque seconde qui passe, toutes les communications seraient écoutées par la NSA : téléphone, fax, e-mails… Comment les trier et les exploiter ? Lorsque le cerveau humain est impuissant, l'ordinateur rend le relais… Et pas n'importe lequel… Des super-calculateurs américains -les SUPER CRAY- sont fabriqués sur mesure pour les besoins de la NSA. Ce sont des bêtes de course à la mémoire sans limite, ils sont également utilisés par l'armée américaine. De cette façon, les conversations téléphoniques sont interceptées et analysées par ces ordinateurs en temps réel. Lorsque les CRAY détectent un mot-clé suspect, la conversation est enregistrée et épluchée par des agents.

> Les ordinateurs CRAY analysent les mots-clés suspects

Pour commencer le processus de tri, tous les signaux des communications (téléphone, fax, e-mails…) sont convertis en langage numérique (binaire, des 0 et des 1). Ainsi, la matière première peut être traitée par les ordinateurs. C'est à ce moment-là que les « dictionnaires » entrent en action. Ce sont d'immenses bases de données dans lesquelles sont stockés des mots-clés, des critères de sélection : noms communs, noms propres, numéros de téléphone, adresses… Régulièrement, tous les trois ou quatre jours, les techniciens de la NSA des cinq pays fondateurs mettent à jour ces bases de données, ajoutent et suppriment des critères, en fonction des informations politiques, diplomatiques et économiques qui leur sont transmises.



Les ordinateurs SUPER-CRAY sont réputés pour être les plus puissants calculateurs qui existent. Au sein du réseau ECHELON, ils analysent toutes les communications en temps réel pour en extraire des mots-clés.

Le principe peut être comparé à celui des moteurs de recherche, sur le Web. Sur Internet, des robots scrutent les sites, ramassent des mots-clés et les ramènent au moteur qui les analysera. Ensuite, c'est au tour des techniciens de prendre la relève des ordinateurs. Ils analysent le produit du tri informatique et ils repèrent les informations sensibles. L'efficacité d'ECHELON réside dans sa puissance de traitement, les ordinateurs CRAY travaillent en temps réel et leurs processeurs sont dédiés à une seule et unique tâche : l'analyse de mots-clés suspects. Pourtant, cette puissance pourrait avoir des failles. De farouches défenseurs de la vie privée diffusent des parades sur le Web. Un exemple, si des milliers d'e-mails sont envoyés en même temps par les internautes et qu'ils contiennent des mots-clés intéressants les ordinateurs de la NSA, le système pourrait être saturé pendant quelques heures. Les exemples de mots-clés sont World domination, Cuba, Jose Bove, CIA, Saddam… Ce type de raisonnement suffit peut être à rassurer les opposants d'ECHELON mais ils sous-estiment certainement les capacités des CRAY. A ce sujet, Duncan Campbell, le « spécialiste » d'ECHELON qui tente d'en savoir plus depuis des années, a précisé que : « des listes de mots-clés hypothétiques (…) seront reconnues en tant que « bruit » et, par conséquent, non traitées ». Ainsi, les tentatives d'embouteillages des internautes du monde entier n'arriveraient qu'à provoquer des fous rires de la part des ingénieurs de la NSA !

> Si des millions d'internautes se mettaient à utiliser PGP...

Au premier abord, la seule parade consisterait à utiliser des outils de cryptage du type PGP. Là, les internautes compliquent effectivement le travail des ordinateurs car ces derniers ont du mal à décoder certains algorithmes. Si vous envoyez un e-mail qui contient un document Word crypté, par exemple, aucun mot-clé n'apparaît. Par contre, l'ordinateur pourra détecter la présence d'un document crypté et il le signalera. Ce sera ensuite au tour des techniciens d'intervenir et de décider s'ils tentent de décrypter le document, ce qui les obligera à utiliser d'autres ordinateurs, en fonction de l'outil utilisé. Certains logiciels de cryptage sont - paraît-il ! - incassables… Que ce soit vrai ou non, cet e-mail aura considérablement compliqué la tâche des analystes et ils auront perdu quelques minutes, voire quelques heures. Tout ça pour finalement lire une déclaration d'amour un peu grivoise ! Plus sérieusement, on peut penser que la NSA pourrait commencer à être ennuyée si des millions d'internautes se mettaient à utiliser des outils de cryptage pour coder tous leurs e-mails. Est-ce pour cette raison que l'utilisation de PGP est réglementée dans de nombreux pays, voire interdite ?

Sur cette question de l'encodage, en 1998, le Parlement Européen a adopté une position plutôt surprenante dans la conclusion d'une note concernant la NSA, au sein d'un rapport disponible sur le site de l'Union qui a pour titre Une évaluation des techniques de contrôle politique (www.europarl.eu.int): « (…) le Parlement européen doit agir pour s'assurer que ces puissants systèmes de surveillance opèrent de façon plus démocratique dès lors qu'il a été mis fin à la guerre froide. (…) Aucune autorité digne de ce nom aux États-Unis n'autoriserait qu'un tel système d'espionnage européen opère à partir du sol américain sans strictes limitations, si tant est qu'elle le fasse. Après un large débat sur les incidences du fonctionnement de

Les grandes dates de la NSA

ECHELON

1986 — Le journaliste d'investigation Duncan Campbell fait les premières révélations à propos du réseau ECHELON.

1988 — La chute du Mur de Berlin redéfinit les objectifs d'ECHELON; les enjeux seront désormais économiques.

1989 — Les antennes de Hong-Kong sont démantelées et transférées en Australie.

1990

1991

1992

1993

1994

1995

1996

1997 — Le Parlement européen souligne la menace que représente ECHELON sur les entreprises européennes.

1998

1999

2000 — le 5 janvier, l'ordinateur central d'ECHELON est hors service à cause du Bug de l'an 2000.

Le siège de la NSA, situé à Fort Meade aux Etats-Unis-, est une base surprotégée par l'armée. Toutes les informations venant du monde entier sont traitées dans ces bâtiments.

ce type de réseaux, le Parlement européen est invité à procéder à un audit indépendant approprié et à contrôler les procédures. Toute tentative visant à proscrire l'encodage par les citoyens de l'Union doit être rejetée jusqu'à la mise en place de systèmes démocratiques et responsables. »

> Toutes les communications et les e-mails sont interceptés

Si on se réfère à ces propos, les citoyens de l'Union sont ainsi invités à utiliser des dispositifs d'encodage tant qu'un « système démocratique » ne sera pas mis en place. Une position ferme puisque l'Union européenne sous-entend clairement qu'ECHELON est un système anti-démocratique qui bafoue allègrement les règles élémentaires des libertés publiques. Si on analyse froidement la situation, la position de l'Union européenne n'est pas très confortable puisqu'un des principaux pays membre de la NSA – la Grande-Bretagne – est également membre de l'Union ! On voit mal comment les Britanniques pourraient prendre une position hostile vis-à-vis de la NSA. Dans ce même rapport du Parlement européen sur « Les techniques de contrôle politique », de nombreux points fondamentaux sont mis à jour officiellement. Premièrement, les auteurs affirment clairement que « toutes les communications électroniques, téléphoniques et par fax (NDLR : de l'Union européenne) sont quotidiennement interceptées par la NSA. » Deuxièmement, il est dit que ces interceptions sont pratiquées pour recueillir essentiellement des renseignements à caractère économique depuis la fin de la Guerre froide. Troisièmement, le rapport précise que selon Privacy International, la Grande-Bretagne est un contrevenant en vertu du Traité de Maastricht, car ce dernier « fait obligation aux États membres de s'informer mutuellement et de se concerter au sein du Conseil sur toute question de politique étrangère et de sécurité présentant un intérêt général ». Or, en vertu des relations particulières de la Grande-Bretagne avec la NSA, les Anglais ne peuvent s'engager à consulter librement leurs autres partenaires européens. Enfin, ce détail technique n'embarrasse que l'Europe, et les Américains continuent à être les premiers informés des derniers rebondissements.

Toujours dans ce fameux rapport du Parlement, nous pouvons donc apprendre que les Européens qui ne font pas partie de la NSA ont connu quelques mésaventures… C'est notamment le cas de la France qui aurait perdu un contrat important (1,4 million de dollars) en 1994, par l'intermédiaire de Thompson-CSF. La célèbre entreprise électronique devait fournir un système radar au Brésil, les négociations étaient bien parties et ce fut finalement la société américaine Raytheon qui obtint le marché. Ce changement de cap fut le résultat d'indiscrétions de la NSA qui fournit le détail des négociations au fabricant américain (source : Sunday Times).

> Airbus perd un contrat de 6 milliards de dollars au profit de Boeing

Autre exemple, la même année, Airbus Industries perd un contrat de 6 milliards de dollars avec l'Arabie Saoudite. Les communications téléphoniques et les fax auraient été interceptés, une fois de plus, par la NSA, au profit de Boeing qui emporte le contrat. Ces exemples sont nombreux, que ce soit en France ou ailleurs, et la NSA préfère mettre en avant des coups d'éclat plus valorisants pour sa paroisse. Ainsi, en 1991, plus de 12 tonnes de cocaïne sont saisies par les Américains grâce à des informations interceptées par la NSA, à partir du Venezuela. Malheureusement, ce type d'exemple est bien plus rare que les histoires de contrats récupérés in extremis par les Américains !

Faut-il voir, dans cette évolution du rôle joué par ECHELON, une redéfinition des principes fondamentaux du capitalisme ? En clair, les Américains auraient-ils mieux compris que nous que la bataille du XXIe siècle sera essentiellement informative et économique ? En maîtrisant les techniques de l'information et de l'écoute, en les mettant au service des entreprises, les Etats-Unis sont-ils en train de prendre une avance considérable sur les autres pays développés non-membres de la NSA ? C'est difficile à dire aujourd'hui, car de nombreuses sources affirment que l'affaire ECHELON est un faux scandale. En fait, la France aurait également signé un accord avec la NSA et nos services secrets profiteraient largement des informations interceptées. Un ancien commissaire de la DST a déclaré que la France était

Les bases qui collaborent avec la NSA au projet ECHELON sont de plus en plus nombreuses dans le monde : ici, la station de Skibsbylejren au Danemark.

prévenue par les Etats-Unis lorsque des risques terroristes planaient. Pour les Américains, la France n'a pas d'autre choix que de coopérer, notre système d'écoute serait archaïque et il nous faudrait des années et des milliards de dollars pour concurrencer la NSA ! **Les ministères français ont beau bénéficier de fonds secrets, il faudrait effectivement quelques dizaines d'années d'économies avant de pouvoir s'aligner… Alors, à vos tirelires !**


L'AMÉRIQUE TOUCHÉE EN PLEIN CŒUR
PHILIPPE TASTET
LES TERRORISTES AURAIENT APPRIS À PILOTER DANS LES ÉCOLES AMÉRICAINES
C'ÉTAIENT NOS PLUS MAUVAIS ÉLÈVES !
PHILIPPE TASTET
VIGIPIRATE RÉACTIVÉ
ÇA ARRÊTE AUSSI LES BOEING ?
ÉCOLE
PHILIPPE TASTET
NOUS SOMMES TOUS DES AMÉRICAINS...
LÀ... TU POUSSES UN PEU LOIN, MEC !
PHILIPPE TASTET
Parce que
nous pensons
que de tristes
sires comme les
terroristes
ne valent pas
la peine qu'on se fasse
du mauvais sang à cause d'eux,
nous,
on a pris le parti d'en rire.
La solidarité ce n'est pas que
le chagrin et la compassion,
c'est aussi l'envie de continuer
et garder l'espoir !