

Découvrez tout l'univers de the hackademy

Publications

Ecoles de hacking et sécurité informatique

Cours par correspondance

CD-rom

Site web



www.thehackademy.net

the HACKADEMY mini PRATIK



Est une publication D.M.P.,
26 bis, rue Jeanne d'Arc.
94160 Saint-Mandé
Tél.: 01 53 66 95 28
Fax : 01 43 98 23 50
RCS PARIS B 391 584 687

DIRECTEUR DE LA RÉDACTION :
Fozzy

RÉDACTION : PROXY & HACKADEMY TEAM

ILLUSTRATION : LECHAKITU

MAQUETTE :
WEEL

CONTACT :
voice@dmpfrance.com
abonnements@dmpfrance.com

IMPRIMÉ PAR ROTOCHAMPAGNE
PRINTED IN FRANCE

DIRECTEUR DE LA PUBLICATION :
O. Spinelli

© 2003 DMP

SOMMAIRE

6	INTRODUCTION
9	LE NAVIGATEUR WEB
16	LES PROXIES OU COMMENT ÊTRE ANONYME SUR LE WEB
28	UNE MESSAGERIE SÉCURISÉE
33	ENVOYER ET RECEVOIR DES MAILS ANONYMES
50	LES LOGICIELS "PEER TO PEER" DE PARTAGE DE FICHIERS
56	CHATTER SUR IRC
58	TÉLÉCHARGEMENT PAR FTP
60	WINDOWS, VOTRE PIRE ENNEMI ?
72	SE DÉBARRASSER DES MOUCHARDS DE MICROSOFT

INTRODUCTION

QUAND ON PARLE DE SURF ANONYME, CERTAINES PERSONNES RÉPONDENT "FACILE, METS UN PROXY DANS TON NAVIGATEUR ET LE TOUR EST JOUÉ !". MALHEUREUSEMENT, CELA EST TRÈS INSUFFISANT POUR GARANTIR UN ANONYMAT TOTAL SUR INTERNET.

LES OBJECTIFS DE CE GUIDE

Le but de ce guide sera atteint lorsque vous aurez assimilé les différentes combinaisons de logiciels et de configurations utilisables pour garantir votre anonymat, et que vous-même serez en mesure d'en trouver d'autres en fonction de vos besoins.

Le site de l'Electronic Frontier Foundation, les grands défenseurs des libertés individuelles sur Internet, propose douze lignes de conduite pour améliorer son anonymat sur Internet (voir la page web http://www.bugbrother.com/eff/eff_privacy_top_12.html) :

- 1 • Ne révélez jamais d'information personnelle par inadvertance.
- 2 • Prenez en main la gestion des cookies.
- 3 • Gardez une adresse e-mail "propre".
- 4 • Ne révélez jamais de détails personnels à des inconnus.
- 5 • Sachez que vous pouvez être surveillés au travail.
- 6 • Prenez garde aux sites qui offrent prix & récompenses en échange de votre contact ou de toute autre information.
- 7 • Ne répondez jamais, et sous aucun prétexte, aux spammeurs.
- 8 • Soyez conscient des enjeux liés à la sécurité sur le Web.
- 9 • Soyez conscient du degré de sécurité de votre ordinateur personnel.
- 10 • Examinez les chartes de protection des données personnelles, et leurs "labels".
- 11 • Rappelez-vous que c'est VOUS qui décidez quelles informations vous révélez sur vous-même, quand, pourquoi et à qui.
- 12 • Mettez-vous à la cryptographie !

Ces règles sont très bonnes, mais insuffisantes pour garantir concrètement que vous n'aurez pas de problèmes. En effet, le bon sens et la paranoïa ne suffisent pas ! Il est absolument nécessaire de pouvoir :

- comprendre, en pratique, ce qui se passe sur le réseau, quelles sont les informations, vous concernant, que peut recueillir un adversaire et comment agir pour l'en empêcher

- mettre en œuvre certains moyens techniques, par l'utilisation de logiciels bien configurés, pour atteindre les objectifs fixés.

Ce sont les raisons d'être de ce mini guide pratique, dont les différents articles sont chacun dédiés à un service Internet (web, irc, ftp, peer 2 peer...) ou un ensemble de programmes (courrier électronique, navigateur, système d'exploitation...). Nous espérons qu'il comblera vos attentes.

POURQUOI RECHERCHER L'ANONYMAT ?

Quand on parle ici d'anonymat, il s'agit plus concrètement de la protection des données pouvant permettre l'identification d'une personne connectée à Internet, et qui utilise un ou plusieurs services distants sur le réseau. L'objectif est tout simplement de protéger ses données personnelles, afin que les personnes (inconnues) avec qui on communique sur Internet ne puissent pas obtenir plus d'informations que ce que l'on veut bien leur donner.

Dans l'anonymat, nous incluons aussi le camouflage de son adresse IP réelle (qui sert à identifier de manière unique n'importe quel ordinateur connecté à Internet).

Les risques d'un manque d'anonymat sur Internet sont variés, et dépendent de vos besoins. Parmi les menaces courantes, citons les spammeurs, les sociétés de marketing commercial, les pirates informatiques, les concurrents, les sociétés d'intelligence économique, les "corbeaux" ou maîtres chanteurs, les consortiums anti-piratage... Et pour les vrais paranoïaques : le complot mondial, la NSA, les services secrets israéliens, Al Qaeda, et les martiens.

On peut aussi penser que, tout simplement, on puisse avoir envie de se balader tranquillement où l'on veut sans être en permanence fliqué, fiché et analysé.

SÉCURISATION

Ce guide suppose que vous démarrez sur une configuration saine, donc sans virus ou troyens sur votre PC, et que celui-ci est sécurisé à l'aide d'un firewall, d'un antivirus et autres anti-espions. Car il serait utopique de dire que vous êtes anonyme si votre disque dur est en possession d'un virus, dialer, cheval de Troie, voire d'un keylogger. Pas plus bavards que ces bestioles là !

Dans un prochain Mini Pratik de The Hackademy, nous expliquerons en détail comment sécuriser un poste sous Windows. En attendant, nous vous conseillons Kerio

comme firewall. Antivir comme antivirus, SpyBot comme tueur d'espions ainsi que SpywareBlaster pour prévenir contre toute intrusion d'espion. Ces logiciels gratuits feront bien le travail, voire mieux que certains logiciels payants.

MISE EN GARDE

Ce guide pratique a été créé pour vous présenter les possibilités techniques utilisables pour la préservation de votre vie privée, et ce dans le cadre et le respect de la loi. Toute utilisation détournée pourra se retourner contre vous si vous effectuez un acte délictueux. Car, si vous serez bien anonymes pour les sites que vous visiterez, vous ne le serez pas pour votre fournisseur d'accès Internet (F.A.I.).

En effet, pour vous connecter, il vous faudra vous identifier auprès de son serveur, et toutes vos connexions transiteront par son réseau... Les forces de l'ordre sont donc parfaitement capables de vous surveiller en écoutant votre ligne téléphonique ou en s'interfaçant au niveau de votre F.A.I.



LE NAVIGATEUR WEB

LA PREMIÈRE DES CHOSSES À FAIRE POUR DÉBUTER DANS L'ANONYMAT, C'EST DE NE PLUS UTILISER LE NAVIGATEUR INTÉGRÉ DE MICROSOFT : INTERNET EXPLORER. ET DE CONFIGURER CORRECTEMENT LES OPTIONS DE VOTRE NAVIGATEUR POUR ÉLIMINER LES COOKIES, LES ACTIVE X ET AUTRES DANGEROUSITÉS.

POURQUOI SE DÉBARRASSER D'INTERNET EXPLORER ?

Parce qu'il est truffé de failles de sécurité non corrigées, dont certaines sont connues depuis plus d'un an. Certains passionnés en sécurité informatique ont signalé ces trous, tel Guninski et http-équiv, mais Microsoft ne fait rien pour protéger les utilisateurs que nous sommes. Malgré leurs bonnes paroles et la sortie régulière de "patches" (correctifs), Internet Explorer (I.E.) reste un véritable gruyère. À l'heure où nous écrivons, il existe un moyen simple, publié sur Internet et utilisé par plusieurs virus, qui permet d'exécuter un code malveillant (cheval de Troie, virus...) sur l'ordinateur de n'importe quelle personne qui surferait avec I.E sur le site web de l'attaquant.

Dans ce cas de figure, si un pirate arrive à exécuter un programme sur votre machine, il a également accès en lecture et en écriture à tous les documents de votre disque dur. Autant dire que vous pouvez faire une croix sur votre anonymat !

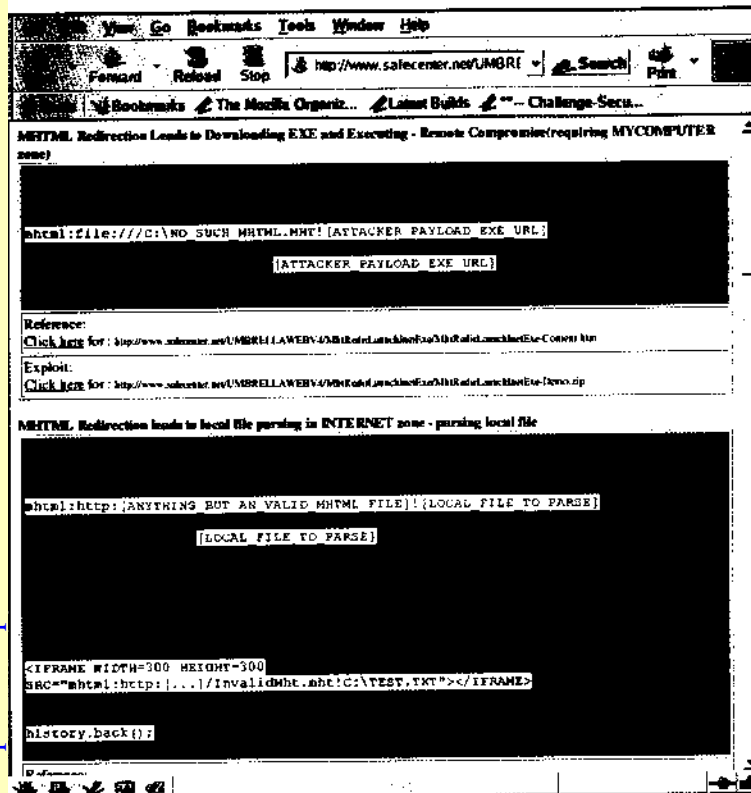
D'autres trous de sécurité, moins importants, permettent de voler les cookies de l'internaute, de lire le contenu de son presse-papier, etc. Ce genre de problème affecte aussi parfois d'autres navigateurs, mais pas de manière aussi chronique, et leurs éditeurs sont plus réactifs pour la publication de correctifs.

Pour plus d'informations, se reporter aux pages web des chercheurs qui ont découvert les principaux trous de sécurité d'Internet Explorer :

<http://continue.to/trie>

<http://www.malware.com/>

<http://www.guninski.com/browsers.html>



Raison supplémentaire, certains composants utilisés par ce programme, tels mshtml.dll (la visionneuse html), Mshta.exe, et l'application d'aide de Windows, permettent d'exécuter des scripts et des fonctionnalités avancées (Javascript, Visual Basic Script, programmes ActiveX, etc...). D'autres trous de sécurité y sont souvent découverts, qui peuvent permettre des actions malveillantes envers vous et vos données. Le pirate, voire le webmaster malhonnête, aura accès libre, par votre navigateur, à vos renseignements personnels et toute donnée sensible vous concernant présente sur votre ordinateur (N° carte bleue /code de connexion...).

Du fait que Microsoft ne propose pas suffisamment de "rustines" comblant les manques de sécurité de ces programmes, I.E. devient manipulable, que ce soit par une personne bien intentionnée ou par un individu malhonnête tel un pirate. Voire par une société de publicité peu scrupuleuse, qui détournera à des fins commerciales les trous de sécurité du navigateur pour vous proposer de la publicité à profusion (installation d'un "adware" sur votre machine).

Enfin, il faut savoir qu'Internet Explorer exporte ses routines dans des fichiers partagés (les fameuses DLL), qui sont intégrés au système d'exploitation de Microsoft. De nombreux logiciels, plutôt que de réinventer la roue, utilisent les fichiers d'Internet Explorer pour faire tourner leurs applications qui nécessitent l'affichage de code HTML. Il est évident que vous ne serez jamais en sécurité si vous les utilisez, puisque ces programmes sont vulnérables aux mêmes failles de sécurité qu'Internet Explorer ! Exemples parmi les logiciels de messagerie : Outlook, Outlook Express, Eudora (désactivable dans les options)...

DIFFICILE DE DÉSINSTALLER INTERNET EXPLORER

Par conséquent, nous vous invitons fortement à bannir l'usage de ce navigateur. Le mieux serait de le désinstaller complètement, mais Microsoft n'a pas prévu cette possibilité !

La suppression d'I.E. est parfois possible, mais nécessite l'usage d'un logiciel dédié à cette tâche. IEradicator (logiciel gratuit) et LitePC (programme payant), du même éditeur, nettoient votre Windows avec efficacité. Le premier n'enlève "que" le navigateur de Microsoft, alors que le deuxième va plus en profondeur en supprimant des programmes non indispensables (et non sécurisés) tel Windows Média Player.

URL : <http://www.litepc.com>

Nous n'allons pas traiter cette procédure en détail. Vous aurez besoin d'être habitué aux manipulations "informaticiennes" afin de compléter le ravalement de votre système, ou bien d'être assisté par un utilisateur plus expérimenté. Par exemple, vu qu'il vous faut désinstaller Outlook Express avant Internet Explorer, vous aurez besoin d'outils efficaces de nettoyage du système et de la base de registres pour cette opération chirurgicale...

S'il est possible d'enlever Internet Explorer sur Win98, 98SE et Millenium, ainsi que sur Windows 2000 SP1, sur toute version supérieure de Windows 2000 et XP cela n'est pas encore le cas. En effet, Microsoft fait en sorte d'enchevêtrer profondément le navigateur avec le système d'exploitation afin d'empêcher toute manœuvre de la part des utilisateurs.

Sur XP, Microsoft a pourtant certifié aux utilisateurs et autres instances américaines de laisser le choix du navigateur en proposant la désinstallation de leur "browser". Bitou a promis, mais ce n'est que du vent : en effet, la commande de désinstallation fait uniquement disparaître les liens vers I.E. situés sur le bureau, mais n'agit en rien sur la suppression d'Internet Explorer qui reste bien tapi dans le système.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia) <http://www.pdfmail.com>

SÉCURISER I.E... EN LE BLOQUANT !

Il existe des astuces pour régler plus finement les options de sécurité du navigateur. En particulier, en décochant "l'Active Scripting" dans les options de sécurité (ou en mettant le niveau de sécurité au plus haut), et en décochant le lancement des ActiveX (même signés). Mais cela ne colmatera pas forcément toutes les failles laissées ouvertes, et empêchera le navigateur d'être totalement fonctionnel. Donc, au minimum, nous vous recommandons de mettre Internet Explorer en berne au profit d'un navigateur plus sécurisé.

Vous pouvez bloquer toute tentative de connexion du navigateur vers le web, empêchant ainsi son utilisation par qui que ce soit ! Pour cela, vous avez deux possibilités qui peuvent être combinées. La première est d'utiliser un firewall personnel (comme Kerio) pour bloquer tout accès à Internet pour le programme iexplore.exe. La deuxième est d'appliquer quelques techniques astucieuses que nous donnons maintenant.

- Pour que personne ne télécharge quoique ce soit avec Internet Explorer vous pouvez bloquer tout téléchargement avec Internet Explorer. Pour cela, il faut lancer le programme regedit.exe (taper "regedit" dans Démarrer/Exécuter) et éditer la clé suivante de la base de registre :

```
HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>Internet Settings>Zones>3
```

Cherchez la clé Dword 1803 et mettez-lui la valeur 3.

Valeur:

0 = téléchargement activé

3 = téléchargement désactivé

- Il existe aussi la possibilité de bloquer l'accès aux fichiers internes sur le PC via Internet Explorer, et de permettre uniquement l'affichage des adresses Internet. Pour cela, éditez la clé suivante dans la base de registre, toujours avec le programme regedit :

```
HKEY_LOCAL_MACHINE>Software>Microsoft>Windows>CurrentVersion>Policies>Explorer
```

Créez une clé Dword ayant le nom NoFileUrl (si elle n'y est pas déjà), et mettez-la à 1 pour bloquer l'accès aux fichiers avec I.E.

Pour plus de sécurité vous pouvez cumuler le tout avec cette astuce :

- Bloquer toute connexion en spécifiant un paramètre de proxy non valide (en fait votre propre adresse IP locale). Allez dans les options d'I.E. et à la section "proxy" vous y entrez l'adresse : 127.0.0.1. Pour le port vous mettez le 3128 par exemple.... et hop le tour est joué !)

Même si une tierce personne utilise votre PC en votre absence, elle ne pourra pas se connecter avec Internet Explorer puisqu'il sera restreint de tous les côtés, et se rabattra sur un autre navigateur. Ces astuces ont aussi l'intérêt de bloquer les programmes malveillants comme les chevaux de Troie ou les adwares qui essaient de se connecter à Internet en passant par I.E.

QUEL NAVIGATEUR CHOISIR ?

Le choix des navigateurs est là, bien présent, et je vous invite à télécharger un de ces "browsers" gratuits, sûrs et fiables qui peuvent remplacer avantageusement Internet Explorer. Vous pouvez même en utiliser plusieurs, cela n'est pas du tout incompatible, sauf pour Netscape et Mozilla qui entrent en conflit.

Vous avez :

- **Mozilla**, dont la dernière version 1.4 sera la dernière et ce au profit de FireBird. Il se télécharge sur :

<http://www.mozilla.org>

Les versions françaises sont disponibles directement ici :

<http://frenchmozilla.sourceforge.net/>

- **BÉONEX**, un clone de Mozilla, au look un peu ancien mais dont les options de sécurité sont très affûtées.

Exemple :

1) élimine tous les cookies lors de sa fermeture (qui se sont installés à votre insu pendant chaque surf).

2) peut bloquer le champ Referrer (l'adresse de la page précédente que vous avez visitée est habituellement envoyée au site web). Voire en envoyer un... faux, bien sûr.

3) bloque les scripts litigieux en HTML.

4) il est léger puisqu'il ne contient pas de messagerie comme Mozilla, et est très stable.

Téléchargez beonex sur :

<http://www.beonex.com>

- **FIREBIRD**, qui est en passe de devenir le navigateur intégré dans la nouvelle suite nommée Mozilla et dont la dernière version est pleine de fonctionnalités impressionnantes :

<http://www.mozilla.org/projects/firebird/index.html>

<http://frenchmozilla.sourceforge.net/firebird/>

<http://frenchmozilla.sourceforge.net/FTP/MOZFIREBIRD/MozillaFirebird-0.6.1-fr-FR-win32.zip>

En ajoutant des plug-ins, il peut lui aussi leurrer les serveurs web que vous visitez. À télécharger sur :

<http://texturizer.net/firebird/extensions.html>

- **OPERA**, qui, s'il comporte dans sa version gratuite une bannière de publicité, est d'une redoutable rapidité et efficacité. Toutefois, je mets un bémol sur les versions 7x que je trouve remplies de fioritures... je suis donc resté sur la version 6.06 en langue française. Parfois nouveautés et beauté ne riment pas avec sécurité, mais chacun ses goûts.

<http://www.opera.com>

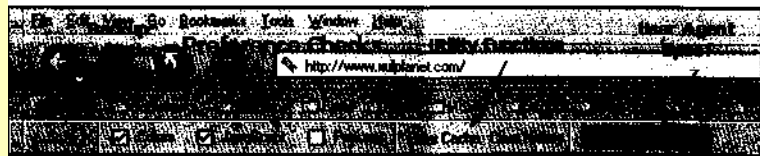
Avec l'un de ces navigateurs gratuits, vous serez beaucoup plus à l'abri pendant vos surfs que derrière Internet Explorer. Lors de la première utilisation de votre nouveau navigateur, vous accepterez donc d'utiliser celui-ci en tant que navigateur par défaut.

Si vous utilisez Béonex, FireBird ou Mozilla, nous vous recommandons chaudement un plug-in qui vous permettra de faire croire au serveur visité que vous utilisez un autre navigateur, et que vous êtes sous un système d'exploitation différent comme Linux ou MacOS. Il s'agit de "La Barre de Préférences/Prefbar" que vous trouverez ici:

<http://www.xulplanet.com>

ou sa page directe :

<http://prefbar.mozdev.org>



Cette barre vous permettra, entre autres, de duper les sites web visités en faisant passer votre système d'exploitation et votre navigateur pour un autre (ex: de Mozilla sous Windows 98, vous tromperez le serveur comme si vous étiez en Netscape sous Linux). Mais vous pourrez aussi tuer les publicités en flash, supprimer les fichiers

temporaires présents sur votre disque dur, et autres options de sécurité/rapidité plus ou moins intéressantes comme la suppression des images des pages web lorsque vous surfez.

Si cette barre fonctionne sans aucun souci sous Béonex et Mozilla, sous les dernières versions de FireBird elle peut occasionner des soucis, donc à éviter avec ce navigateur.

Bonus : si vous trouvez votre Béonex tristounet, mettez la barre de préférences sous Mozilla 1 et l'O.S. en Windows 98, et visitez le site suivant qui vous propose d'habiller joliment votre navigateur :

<http://mozdev.org>

À noter qu'il existe un navigateur dénommé "Ghost", dédié à l'anonymat, qui cache votre adresse IP ainsi que vos différentes infos personnelles. Ce programme pourrait vous satisfaire, mais il utilise certaines DLL d'Internet Explorer ! Donc, le jour où ce browser sera autonome dans son fonctionnement, nous pourrions vous le conseiller.

CONCLUSION

N'omettez pas de configurer finement la sécurité de votre navigateur. Les options sont utiles, alors jetez-y un petit coup d'œil :

- cookies et historique à jeter fréquemment, voire à chaque session.
- fausses informations personnelles ou mieux encore... aucune !
- pas de téléchargement sans votre autorisation.
- élimination fréquente des fichiers temporaires (cache), voire mieux : élimination automatique à la fermeture de votre navigateur.
- ne pas accepter d'utiliser SSL v2 qui n'est sécurisé (SSL v3 et TLS sont OK).
- si vous n'avez pas peur de perdre des fonctionnalités, refusez les applets java et le javascript.

Intervenir sur le navigateur et éliminer Internet Explorer permet en partie de limiter la diffusion de vos infos personnelles. Par contre, vous ne pourrez pas empêcher certains composants de votre système de se connecter à votre insu lors de vos surfs, sans que vous puissiez lutter contre... Quoique ! Lisez la suite pour de plus amples astuces pour préserver votre anonymat.

LES PROXIES, OU COMMENT ÊTRE ANONYME SUR LE WEB

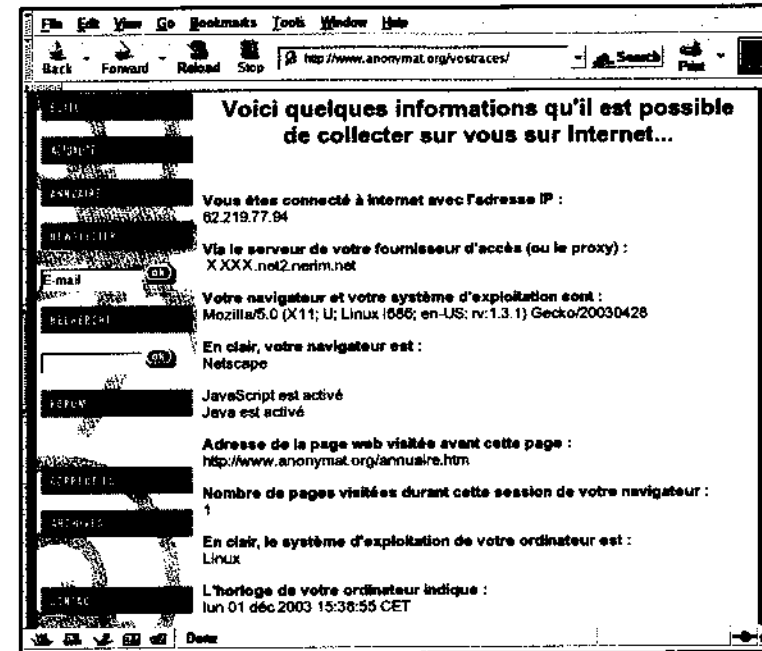
LORSQUE VOUS SURFEZ SUR LE WEB, VOTRE NAVIGATEUR ENVOIE DES INFORMATIONS AUX SITES VISITÉS : COOKIES, PAGE PRÉCÉDENTE, ENTÊTES... ET SURTOUT, VOTRE ADRESSE IP. POUR NE PAS POUVOIR ÊTRE SUIVI À LA TRACE, IL FAUT UTILISER DES PROXIES.

VOS TRACES SUR LE WEB

Effectuons quelques tests afin de contrôler réellement les informations que le navigateur diffuse à tout vent. Lorsque vous vous promenez sur un site quelconque, de nombreuses informations personnelles peuvent être récupérées par le serveur, puis stockées à votre insu. Pour avoir une idée de ce qu'un simple browser peut dévoiler, visitez l'une de ces adresses :

- <http://www.elfqrin.com/binfo.shtml>
- <http://privacy.net/analyze/>
- <http://www.anonymat.org/vostraces>
- <http://www.pcflank.com/> (tests de sécurité)

Vous pouvez également obtenir le même genre d'informations en français sur la fameuse page de la CNIL :
<http://www.cnil.fr/traces/>



Nous vous déconseillons par contre d'effectuer des tests en ligne sur les sites d'éditeurs de logiciels quand ils vous font télécharger des DLL ou des composants ActiveX. Toutes les actions potentiellement nocives de ces programmes ne vous sont pas révélées, alors qu'ils ne possèdent aucune limitation d'intervention sur votre PC. Certains sont sujets à des trous de sécurité. Donc prenez garde lorsque l'on vous propose de télécharger un quelconque programme...

L'information la plus sensible est l'adresse IP, et c'est ce que l'utilisation d'un proxy va permettre de camoufler. Avec votre adresse IP, les webmasters, les fournisseurs d'accès, ou les hébergeurs, peuvent croiser leurs enregistrements et savoir (par exemple) que vous êtes la même personne qui a acheté tel article sur une boutique en ligne, puis qui a posté tels messages à caractère politique sur un forum. De plus, avec une adresse IP, on peut savoir de quelle pays et de quelle ville vous venez, ainsi que le nom de votre fournisseur d'accès. Avec toutes ces informations, remonter à vos noms et prénoms est souvent réalisable. Sur certains fournisseurs d'accès comme Nerim, il est même possible à l'heure où nous écrivons d'obtenir directement le nom et prénom d'un abonné uniquement à partir de son adresse IP, en interrogeant d'une certaine manière un serveur email...

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia) <http://www.pdfmail.com>

LA SOLUTION : LE PROXY

L'outil indispensable que nous allons retrouver à plusieurs reprises, c'est le proxy, mot magique qui fait encore peur à certains. La preuve avec cette perle trouvée sur le forum d'anonymat.org, par une personne dont je respecterai l'anonymat, qui répond à la question "comment fait-on pour être anonymisé ?" (sic) : "d'après ce que j'ai cru comprendre il me faudrait un truc nommé 'proxy', mais lequel (il y en a tout un tas sur les sites américains qui sont proposés, et je n'y comprends rien !), où peut-on télécharger gratuitement ce proxy, et comment l'utiliser ?". Bon, on peut en rire, mais ça montre qu'il y a certaines notions à clarifier.

Un proxy n'est pas un logiciel. Il s'agit d'un nom pour désigner un ordinateur auquel on se connecte, et auquel on demande de faire des opérations à notre place: comme télécharger une page web, et de nous renvoyer le résultat (la page web). Un proxy agit donc comme un intermédiaire entre notre ordinateur et le site, de façon à ce que nous ne soyons jamais connectés directement au site. Notre véritable adresse IP est alors invisible pour le site en question. Fin du tour de magie.

Maintenant, où se trouve ce fameux proxy ? Il en existe en fait des milliers : il s'agit tout simplement de serveurs sur lesquels tourne un logiciel spécial permettant cette fonctionnalité (il existe de nombreux logiciels différents). On peut classer ces serveurs en deux catégories : les proxies "officiels", c'est-à-dire ceux qui sont destinés à cette tâche, et les "officieux", c'est-à-dire ceux qui n'étaient pas initialement prévus pour ça.

Les premiers font de la pub et sont souvent payants, ou très lents s'ils sont gratuits. Les derniers sont des ordinateurs mal configurés, souvent des proxies d'entreprises qui ont oublié de mettre des restrictions sur qui a le droit d'utiliser le proxy. Si personne d'autre que vous n'a découvert leur fonction cachée de proxy, ils peuvent être très rapides, si par contre des centaines d'internautes profitent de leur bande passante, ils peuvent ramer (presque) autant que Windows XP avec 64 Mo de RAM. De plus, ils ne restent que rarement disponibles très longtemps, car l'entreprise finit par se rendre compte d'où vient sa facture de 50000\$ d'excès de bande passante du mois dernier (les proxies sont aussi très utilisés par les spammeurs, de façon à pouvoir envoyer impunément des tonnes d'emails sans craindre de voir leur IP bannie). On peut se demander s'il est illégal d'utiliser un tel proxy. À notre connaissance, non (du moment que vos activités sont légales bien sûr), puisque vous vous contentez d'utiliser un service offert sur la machine (ce n'est pas votre faute si ce service n'aurait pas dû exister). Mais méfiance tout de même, la législation n'est pas claire sur ce sujet !

Certains proxies sont plus anonymes que d'autres. En effet certains proxies web

(HTTP) peuvent transmettre votre adresse IP au site visité. Nous verrons plus tard comment vérifier si c'est le cas. D'autres types de proxies, appelés proxies Socks, sont plus anonymes et plus polyvalents puisqu'ils ne sont pas limités au web :

LES DIFFÉRENTS TYPES DE PROXIES

Vous êtes perdus entre Socks, HTTP, ports 3128 à 8080, etc ? Pas de panique, nous allons éclaircir tout ça. Les proxies "classiques" pour le web sont les proxies HTTP, qui sont utilisés par un navigateur web comme Internet Explorer. Ces proxies ne sont, à la base, pas prévus pour autre chose, et sont presque toujours accessibles sur les ports 8080 ou 3128 (mais aussi parfois 80, ce qui est moins courant dans le cas d'une configuration "normale"). Les proxies Socks, eux, sont plus récents et sont utilisés dans beaucoup plus d'applications, car ils permettent de faire passer n'importe quel trafic Internet et non pas seulement le Web. Les proxies Socks se dénichent presque toujours sur le port 1080. Enfin, une petite subtilité existe : les proxies HTTP qui acceptent le HTTPS (HTTP sécurisé). Utilisés en mode https, ils sont plus anonymes qu'en mode HTTP. Ils peuvent même parfois permettre de faire passer n'importe quelle connexion TCP (IRC par exemple), un peu comme un proxy Socks, avec un logiciel approprié. Et voilà, c'est tout ce que vous avez à savoir pour vous aventurer dans le monde merveilleux des proxies !

tout type de connexion (IRC, peer to peer,

email...) peut être relayé par ces proxies. Finie la théorie, place à la pratique !

LES PROXIES OFFICIELS

Commençons avec le plus simple, les proxies officiels. L'un des plus anciens et des plus connus est Anonymizer (www.anonymizer.com). Vous pouvez l'utiliser très simplement en tapant l'adresse :

http://anon.free.anonymizer.com/http://adresse_a_visiter_anonymement.

Comme adresse à visiter, essayez par exemple celle de la CNIL donnée plus haut pour vérifier que votre adresse IP est bien cachée. Si vous avez un doute sur votre véritable IP, tapez "ipconfig" dans une fenêtre de commandes MS-DOS pour la trouver (pour lancer une invite de commande MS-DOS, faites Démarrer/Exécuter et lancez cmd.exe ou command.com). Malheureusement, dans sa version gratuite, Anonymizer bloque certains sites, comme Hotmail, ou les sites sécurisés utilisant HTTPS. Ce n'est donc pas une solution satisfaisante à 100%.

Un autre service de surf par proxy est "The Cloak" (www.the-cloak.com), mais la version gratuite est également très limitée (elle interdit notamment les commandes POST, c'est-à-dire tout remplissage de formulaire, donc de login sur un site protégé par mot de passe). Finissons les gratuits avec Anonymouse (<http://nonymouse.com/anonwww.html>), entièrement gratuit mais pas très perfectionné. Il existe encore d'autres proxies payants proposant un accès gratuit limité, mais je n'ai rien trouvé de bien sensationnel.

TROUVER SES PROPRES PROXIES

Si vous voulez être libre de vos mouvements, il faudra donc y mettre un peu du vôtre, et vous trouver un proxy par vous-même. Rappelons que nous cherchons un proxy pour le web : par tradition, ces proxies écoutent (reçoivent les requêtes) sur le port 8080, mais on en trouve aussi sur les ports 80 et 3128. Vous pouvez donc utiliser un outil de scan afin de trouver un tel proxy.

Rappelons tout d'abord que scanner consiste à "examiner" un ordinateur pour déterminer quels sont les services qu'il offre. Bien que légale en théorie, cette pratique est souvent considérée comme illégale car étant la première étape d'une tentative de piratage (après avoir scanné et trouvé un logiciel tournant dessus, on peut essayer d'exploiter une faille de ce logiciel pour hacker la machine). Enfin bref, sachez que si vous scannez, votre fournisseur d'accès vous fera peut-être parvenir un jour une lettre vous demandant d'arrêter, et là je vous conseille d'obéir ;) En attendant, scanner permet de découvrir des proxies pour vous tout seul (donc potentiellement rapides). Vous pourrez trouver plusieurs scanners spécialisés dans les proxies en cherchant "proxy scanner" dans google. Pour les flemmards, en voici un par exemple :

<http://www.proxybench.com/proxy/sockschecker.asp>.

Généralement, vous devrez spécifier un intervalle d'adresses IP à scanner, et le programme fera le reste. Je vous conseille d'éviter les adresses d'universités, qui sont reconnues comme très peu douillettes quand on les chatouille avec un scanner (ce qui signifie que ça ne les fait absolument pas rigoler). Et vous savez quoi ? Lorsque vous scannez, vous avez intérêt à passer par un proxy, afin de scanner anonymement !

Vous pouvez essayer de faire plus simple en utilisant des proxies trouvés par d'autres. Il existe sur le net de nombreuses listes de proxies, mais malheureusement la plupart du temps elles ne sont pas à jour et aucun ne fonctionne. Certains programmes viennent aussi avec des listes de proxies censées être mises à jour, mais nous en avons testés pour vous et le résultat est le plus souvent décevant. Celle de SocksChain (voir l'encadré qui lui est consacré) est la meilleure que j'ai trouvée. Une autre est celle du site MultiProxy, sur http://www2.multiproxy.org/anon_list.htm, sur laquelle je suis parvenu à trouver deux proxies fonctionnels (si si !). Du côté des sites de listes de proxies, allez donc faire un tour par exemple sur http://www.stayinvisible.com/index.pl/proxy_list et les liens qui en partent, vous trouverez sans doute votre bonheur.

Quelques autres adresses de sites proposant des listes de proxies :

<http://www.proxyl.com>

<http://tools.rosinstrument.com/proxy/>

<http://proxys4all.cgi.net/>

<http://www.astalavista.com/privacy/library/proxy/proxyserver.shtml>

<http://www.samair.ru/xwww/proxy.htm>

<http://atomintersoft.com/products/alive-proxy/proxy-list/default.asp#proxy-list>

<http://www.cs.nchu.edu.tw/doc/anonymous.html>

Attention, utiliser un proxy "non officiel" n'est pas forcément exempt de tout danger ! Il faut savoir ce que l'on risque, en particulier :

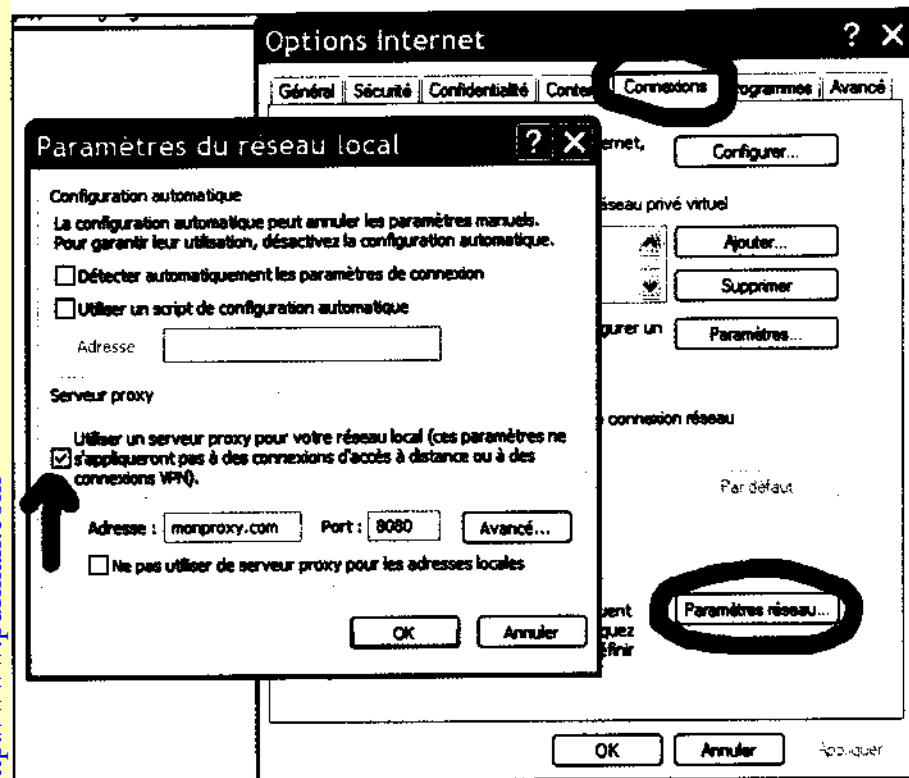
- ces proxies sont souvent moins perfectionnés que les proxies type Anonymizer.com, ne camouflant pas votre système d'exploitation par exemple, ou d'autres informations système. Les proxies payants offrent aussi souvent des fonctions de blocage des scripts "malveillants" (Javascript et compagnie) pour plus de sécurité.
- des logs sont généralement conservés. Si vous faites une bêtise, votre véritable IP pourra donc être retrouvée par le propriétaire du serveur.
- autre problème posé par les logs : vous ne savez pas ce qui est loggué (enregistré). Quelqu'un d'un peu vicieux pourrait très bien s'amuser à configurer un serveur proxy sur sa machine, attendre que quelqu'un le scanne, et alors espionner les utilisateurs.

Nous ne vous conseillons donc pas de vous connecter à des sites nécessitant des mots de passe que vous devez absolument garder confidentiels, ou de rentrer votre numéro de carte bleue lorsque vous utilisez un tel proxy. Le risque, s'il est minime, n'en vaut pas la peine.

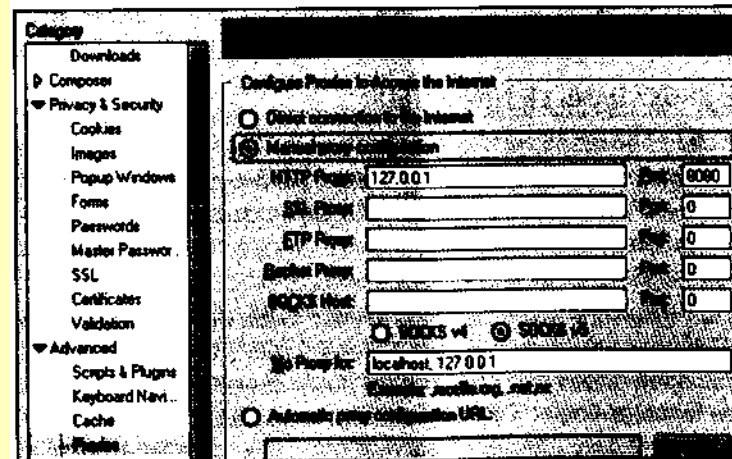
CONFIGURER LE PROXY DANS LE NAVIGATEUR

Maintenant que vous avez un proxy à utiliser (par exemple monproxy.com:8080), il faut encore configurer votre navigateur web pour lui indiquer de passer par le proxy au lieu de se connecter directement aux sites.

- Sous IE, cela se fait (pour une connexion internet par ADSL ou réseau local) en cochant la case "utiliser un serveur proxy..." dans Outils / Options Internet / Connexions / Paramètres réseau (voir capture d'écran). Si vous utilisez un bon vieux modem 56K, dans le même onglet "Connexions" cliquez sur la connexion puis sur "Paramètres" et cochez la case "Utiliser un serveur proxy pour cette connexion".



- Dans Mozilla, Netscape ou FireBird, allez sur la barre de fonctions, cliquez sur "Edit" puis "Préférences" et "Advanced" et pour finir cliquez sur "Proxies".



- En ce qui concerne Opéra, c'est encore plus simple. Appuyez en même temps sur les touches "alt" et "p", ou passez par le biais du menu "fichier" > "préférences". Vous accédez alors à la fenêtre des préférences, dans laquelle vous devrez cliquer sur "réseau". Cliquez ensuite sur le bouton "serveurs proxy". Configurez votre proxy, puis cliquez sur "appliquer" puis sur "ok" qui fermera la fenêtre de "réseau".

VÉRIFIER L'ANONYMAT DU PROXY

Ensuite, il faut vérifier que le proxy est de type "anonyme", c'est-à-dire qu'il ne révèle pas votre adresse IP au site distant (par exemple en lui disant "au fait, c'est untel qui m'a demandé de récupérer cette page web"). Il existe plusieurs méthodes pour vérifier le caractère anonyme d'un proxy, comme le programme MultiProxy, ou à l'aide d'un site web, comme :

http://www.multiproxy.org/env_check.htm

Allez à cette adresse après avoir configuré votre navigateur avec votre proxy, et vérifiez que votre véritable adresse IP n'apparaît nulle part sur la page web.

Pour trouver votre véritable adresse IP, demandez à votre système de vous fournir l'IP en cours de service :

- sur Windows 98, ME :

Démarrer>Exécuter> écrivez " winipcfg "

- sur Windows 2000 & XP :

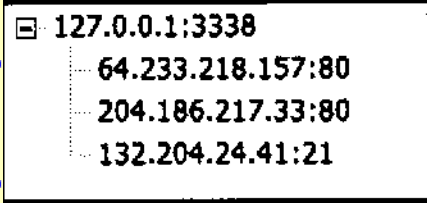
Démarrer>Exécuter> écrivez " cmd " >cliquez OK >ensuite dans la fenêtre écrivez " ipconfig /all "

• Mettez plusieurs paires de chaussettes

SocksChain (<http://www.ufasoft.com/socks/>) est un programme extrêmement utile pour tout internaute parano qui se respecte. Il permet en effet de créer simplement des "chaînes" de proxies : grâce à lui, vous pouvez mettre entre vous et votre cible autant de proxies intermédiaires que vous le souhaitez, ce qui permet de s'assurer d'un anonymat confortable (il faudra beaucoup de temps à une personne très motivée pour remonter une piste de plusieurs proxies depuis les quatre coins du monde).

Comment utiliser ce petit outil ? La première chose à faire est d'aller dans "Tools / Proxy Manager" et de cliquer sur "Update list" pour télécharger la dernière liste de proxies, puis "Test all" pour les vérifier. Ceci fait, fermez le proxy manager puis cliquez sur "Service / New". Dans "Accept connections on Port" nous vous conseillons de mettre autre chose que 1080 pour plus de sécurité. Vous pouvez laisser les autres options identiques ("Change the chain every" permet de spécifier au bout de combien de temps le programme

modifie automatiquement la chaîne pour plus de sécurité. "Chain length" spécifie une longueur de chaîne, et enfin, si vous le souhaitez, vous pouvez choisir quels proxies vous voulez exactement utiliser). Après avoir cliqué sur OK, la chaîne est activée et il suffit de configurer votre logiciel (miRC par exemple) avec comme proxy un proxy Socks (4, à moins que vous n'utilisiez que des Socks 5 dans la chaîne), à l'adresse 127.0.0.1 et sur le port que vous avez spécifié (1081 par exemple). Lorsque vous vous connectez, vous devriez voir en haut à droite de la fenêtre de SocksChain une petite arborescence qui montre les connexions en cours, comme dans la capture d'écran ci-après.



<input checked="" type="checkbox"/>	127.0.0.1:3338
<input type="checkbox"/>	64.233.218.157:80
<input type="checkbox"/>	204.186.217.33:80
<input type="checkbox"/>	132.204.24.41:21

TROMPER LES SERVEURS WEBS AVEC PROXOMITRON

En complément, vous pouvez utiliser un programme de sécurité et d'anonymat entre votre connexion et votre navigateur, comme Proxomitron. C'est le meilleur de ce type de logiciels car, s'il vous protège des scripts vicieux, il peut aussi duper les serveurs web en leur donnant des fausses informations sur vous et votre système d'exploitation. Vous pouvez bien évidemment le configurer pour mettre un proxy externe dans sa base, voire plusieurs qu'il fera tourner successivement.

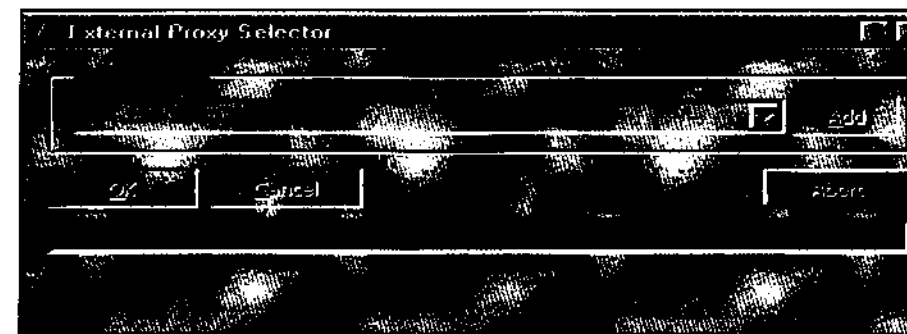
Proxomitron (site américain) :
<http://www.proxomitron.info/>

Sites français qui donnent quelques détails :
<http://www.lipsheim.org/foret/proxomitron.htm>
<http://sebsauvage.net/logiciels/proxomitron.html>

Ce software anglais est d'une efficacité redoutable, mais je vous invite à télécharger son patch de traduction française sur :
<http://www.anticrash.net>

Avec Proxomitron, votre navigateur ne pourra pas révéler vos infos vu qu'il bloquera toute transmission des données sensibles. Vous serez donc encore mieux protégé, même si le proxy externe ne fait aucun travail d'anonymat supplémentaire par lui-même. Par contre, ce logiciel ne peut pas protéger l'adresse IP, c'est là la responsabilité du proxy externe.

Proxomitron contient un testeur de proxies qui vous confirmera que le proxy que vous comptez utiliser est bien en fonction. Toutefois, cela ne vous dispense pas de faire un test pour contrôler le degré "d'anonymisation" de votre connexion. Sur la version anglaise, allez sur "set remote proxies". Dans cette fenêtre vous mettez l'adresse IP de votre proxy, puis les deux points ":", et ensuite le port du proxy, par exemple 8080. Ensuite cliquez sur "test" et Proxomitron lancera le test, qui sera concluant ou pas en fonction du proxy.



Testez le proxy à chaque lancement de logiciel afin de contrôler réellement votre protection... et si la connexion est impossible, sachez que si l'administrateur dudit serveur constate une recrudescence du trafic sur son serveur, il pourra le fermer et vous vous retrouverez à chasser un autre proxy.

Concernant MultiProxy, un logiciel souvent proposé dans les tutoriaux d'anonymat, nous vous le conseillons moins, car en fait ce programme n'assure que la gestion de proxies. En aucun cas, il ne vous protège ni ne vous propose un avertissement si le proxy que vous utilisez n'assure plus votre anonymat. Donc, dans le cas où le proxy se modifierait lors de votre surf ou que celui-ci ne soit pas fiable, MultiProxy ne fera rien pour vous ! Prudence alors si vous désirez continuer à surfer derrière ce programme.

La seule action que vous pouvez faire avant de surfer librement, c'est de tester à plusieurs reprises l'anonymat de votre connexion sur les sites donnés précédemment.

• Configuration

Pour utiliser Proxomitron, il faudra que vous configuriez le navigateur afin que celui-ci utilise Proxomitron comme proxy ! Pour cela, configurez le proxy 127.0.0.1 (cette adresse IP représente toujours votre propre ordinateur) sur le port 8080, de la même manière que celle qui nous a servi à configurer un proxy dans les pages précédentes.

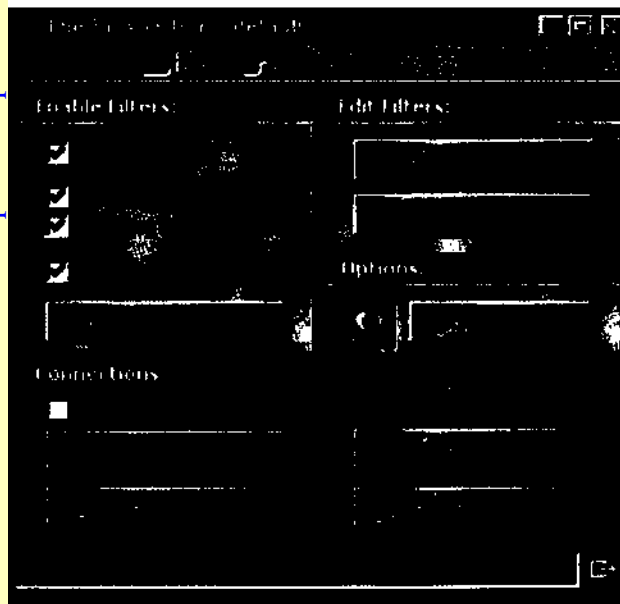
Ensuite, afin que Proxomitron remplisse son office, vous allez le déclencher manuellement puis cliquer sur son icône en forme de triangle vert située dans votre barre des tâches. Faites un clic droit dessus puis cliquez sur "open proxomitron".

Une première fenêtre s'affiche. Il faut que les 3 cases soient bien cochées. En ce qui concerne la quatrième, vous ne pourrez la cocher que si vous avez un serveur proxy externe en fonctionnement. Vous remplirez l'adresse IP du proxy à ce moment, pour que Proxomitron puisse se connecter à ce serveur proxy externe.

Note : une option existante dans Proxomitron vous permet de lancer automatiquement le navigateur que vous aurez choisi pour surfer anonymement, dès l'ouverture de Proxomitron. Pour cela, cliquez sur le bouton "config", puis, dans l'onglet "startup", cochez la case "run entry below when Proxomitron starts", puis recherchez le lien exact de votre navigateur sur votre PC en cliquant sur le petit bouton "find" (donnez le chemin de iexplore.exe pour lancer Internet Explorer, par exemple). À chaque fois que vous lancerez Proxomitron afin de protéger votre surf, le navigateur choisi se mettra lui aussi en route.

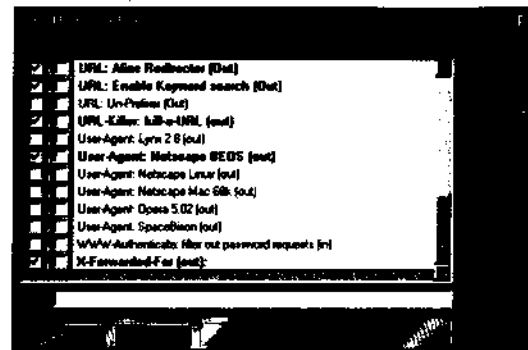
Maintenant nous allons configurer finement Proxomitron afin de tromper l'éventuel petit malin qui tente de vous filer le train !

Pour cacher votre système d'exploitation et votre navigateur, ainsi que leurrer les sites web en leur donnant de fausses informations, il vous faut aller dans "Enable Filters" puis cocher les 4 cases (voir photo d'écran).



Allez ensuite sur "Edit Header Filters", faites glisser la barre de défilement jusqu'en bas, jusqu'aux lignes "Users Agent", et cochez une de ces cases dans la colonne "out". En cochant cette unique case, vous allez faire croire aux espions que vous êtes sous "lynx", ou bien "Opéra", ou Netscape BeOs", voire "Netscape-Linux"... Choisissez ce qui vous plaît afin d'être masqué.

En dernier lieu vous allez cliquer sur la dernière ligne du bas "X-Forwarded-For", toujours du côté "out". Pour finir cliquez sur "Apply" puis sur "OK".



Un dernier petit travail nous attend. Quand vous êtes sur la première fenêtre, cliquez sur le bouton "webpage" puis recherchez les 3 lignes qui se suivent commençant par "hide browsers... from JS". Cochez les trois puis cliquez sur "Apply" et enfin sur le "OK" final.

AUTRES LOGICIELS UTILES

HTTPPort permet de faire passer une connexion TCP quelconque (donc n'importe quelle application utilisant TCP, et non seulement le web) à travers un proxy HTTP. Vous trouverez son aide à la configuration ici :

Vous pouvez télécharger ce logiciel à l'adresse suivante :

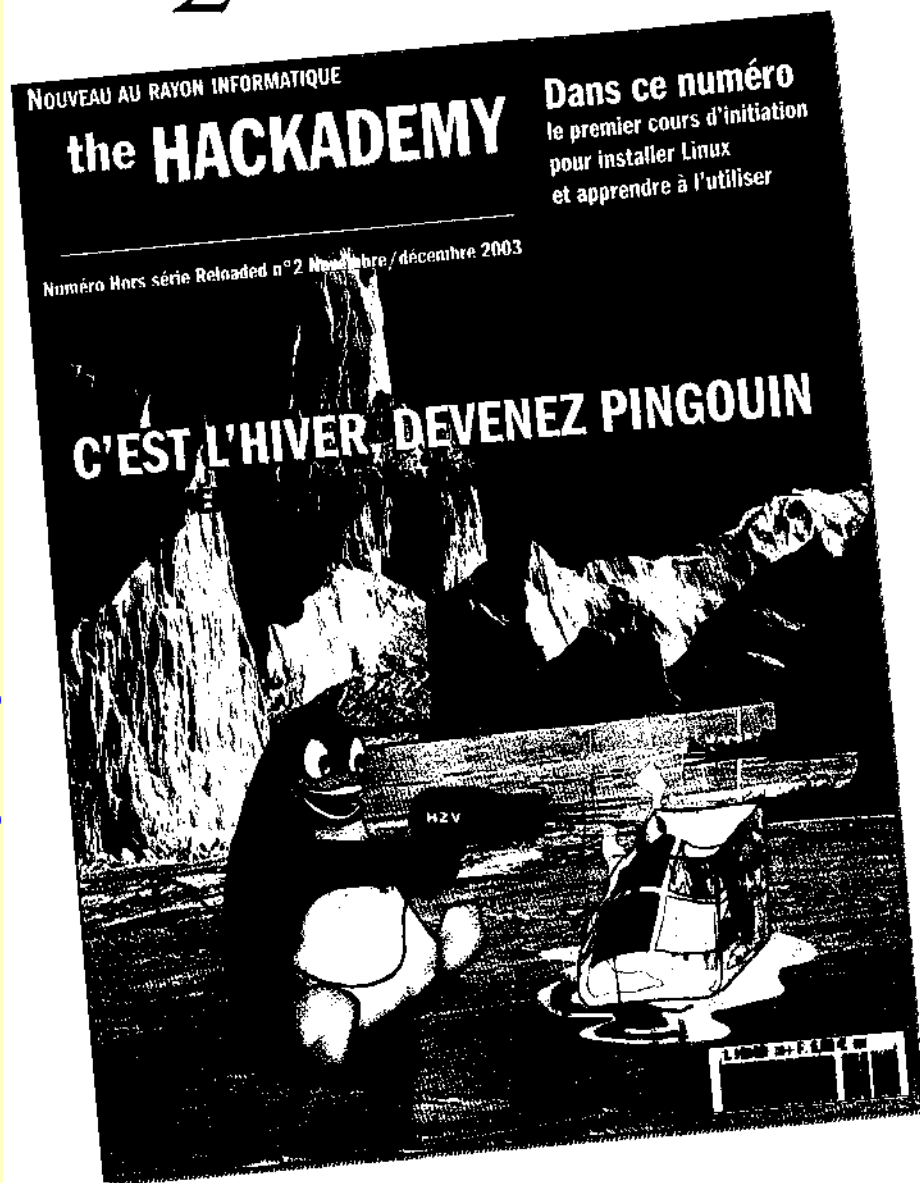
SocksCap permet de lancer n'importe lequel de vos programmes en rendant anonyme sa connexion à Internet (messagerie, messenger direct, jeu, etc...). Il est capable de faire passer la connexion par un proxy Socks, même si le logiciel n'est pas conçu pour utiliser un tel proxy.

Téléchargement sur :

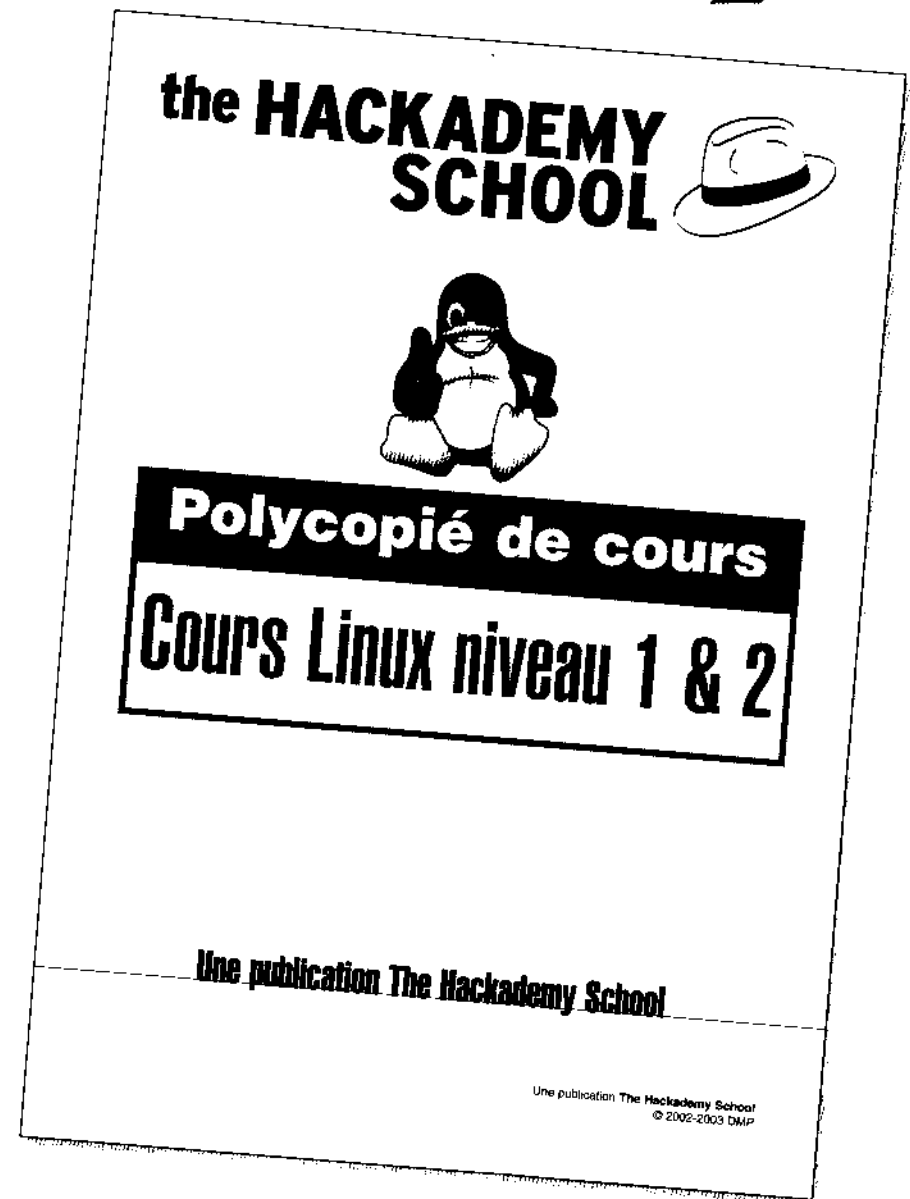
Présentation :

Tutoriel facile:

Explications:



UN HORS SÉRIE POUR PASSER A LINUX
UNIQUEMENT SUR COMMANDE AU 01 53 66 95 28
6,50 € FRAIS DE PORT COMPRIS



LE COURS LINUX DE THE HACKADEMY
CHEZ VOUS! VOIR PAGE 78

UNE MESSAGERIE SÉCURISÉE

AVANT DE S'INTÉRESSER AUX TECHNIQUES AVANCÉES POUR ENVOYER DES E-MAILS ANONYMES, IL EST NÉCESSAIRE DE DISPOSER D'UN LOGICIEL DE MESSAGERIE RELATIVEMENT SÛR. NOUS VERRONS ÉGALEMENT QUELQUES ASTUCES UTILES, ET LES MOYENS DE RÉSOUDRE LE PROBLÈME DU SPAM, CES MESSAGES PUBLICITAIRES QUI NOUS ENVAHISSENT.

REEMPLACER OUTLOOK EXPRESS

Comme Outlook Express utilise les DLL d'Internet Explorer et possède les mêmes paramètres de sécurité (donc souvent les mêmes failles), nous vous proposons de choisir un mailer plus adéquat pour garantir votre sécurité.

Outlook Express utilise la visionneuse de Internet Explorer pour afficher les mails en HTML, et les saletés du Net (scripts divers, ActiveX) incluses dans les messages (pièces jointes et/ou dans le corps du mail) peuvent profiter des failles de l'un et de l'autre pour ouvrir des portes dérobées sur votre ordinateur (backdoors). Abandonnez donc Outlook (Express), et même, désinstallez-le après avoir sauvegardé vos e-mails et carnet d'adresses.

Pour le désinstaller, ne le mettez pas en service, puis dans le "panneau de configuration" accessible par "Paramètres" du "menu de démarrage", double-cliquez sur "Ajout/Suppression de programmes" puis sur "Ajouter/Supprimer des composants windows". Là, vous pourrez cocher Outlook Express, et vous cliquerez sur "Supprimer". Pour finaliser la désinstallation, un petit coup de balai d'un programme quelconque de nettoyage de la Base de Registres permettra d'éliminer les déchets résiduels inutiles.

Ensuite vous pourrez installer un nouveau mailer fiable, sécurisé et tout aussi gratuit.

Vous avez à votre disposition :

- **FoxMail**, qui est très convivial et utilise sa propre visionneuse HTML. Il possède une fonction de recherche des mails sur Hotmail.

<http://foxmail.free.fr>

- **Calypso**, dont les options de sécurité sont impressionnantes contre les virus et les spams, avec le seul bémol qu'en mode HTML il utilise la visionneuse "mshtml.dll" de Microsoft. Mais vous pouvez désactiver cela en mettant la réception et l'émission des mails en mode texte.

<http://www.gratilog.net>

- **ThunderBird**, qui est un composant des groupes tournant avec Mozilla. Il reste en anglais mais devrait se franciser prochainement. D'ailleurs un site français (voir ci-dessous) le propose dans la langue de Molière. Un avantage, il fonctionne sans l'aide d'un fichier de Microsoft. Par contre il pêche encore un peu par sa jeunesse, vu sa lourdeur et sa consommation de ressources, mais ses développeurs passionnés le font évoluer fréquemment.

<http://www.mozilla.org/projects/thunderbird/index.html>

<http://texturizer.net/mozilla/fr/thunderbird/>

• Pourquoi ces 3 programmes ?

Parce que leurs capacités à réagir contre les virus et autres saletés du web sont importantes et qu'ils sont souvent mis à jour par leurs éditeurs respectifs. De plus, ils n'ont pas besoin d'un autre logiciel pour fonctionner, ils sont indépendants... sauf pour Calypso en mode HTML. Et de plus, ils sont gratuits :) Alors, qu'attendez-vous ? Bien sûr, si vous avez Mozilla, vous pouvez utiliser la messagerie intégrée à Moz'. Cela sera toujours plus fiable et sécurisé que par Internet Explorer et Outlook Express.

Indispensable, le programme Dawn (convertisseur de formats) vous permettra de passer d'un mailer à un autre sans perdre vos e-mails :

<http://www.joshie.com/projects/dawn/index.html>

Dernier petit conseil pour cette partie : si vous utilisez un programme dénommé "Incrédimail" ou que vous connaissez quelqu'un qui l'utilise, bannissez ce programme, car il se sert d'Outlook Express pour fonctionner - ce qui n'est pas un gage de sécurité. De plus, c'est un nid à scripts HTML, avec toutes ces images et autres animations à gogo... et tous les problèmes de sécurité potentiels que cela implique. Alors à la trappe, le logiciel de pacotille.

SE PROTÉGER DU SPAM

Vous pouvez ajouter à votre nouveau mailer un programme de filtrage des spams et autres virus. Nous vous conseillons le "tueur de spams" SpamPal, qui comporte plusieurs plug-ins apportant de nombreuses options pour lutter contre toutes les cochonneries du web. Vous trouverez ce programme génial ici : <http://www.spampal.org>

Surtout n'omettez en aucun cas de lui adjoindre le plug-in "HTML modify" qui est le plug-in de filtrage "antisaletés" par excellence. La dernière version (bêta 1.50) est proposée en multilingues, dont le français. Et des passionnés de SpamPal ont créé plusieurs sites en français afin de vous permettre de "dompter" ce superbe programme.

En changeant de messagerie, non seulement vous protégerez vos données contre les virus, mais vous vous mettrez aussi à l'abri des scripts malicieux qui pourraient révéler des infos sur votre système à l'expéditeur du mail. Par contre, si vous désirez garder absolument Outlook Express voire le pire Incrédimail, mettez-leur SpamPal, ça sera au moins une bonne protection... et surtout ne cliquez pas sur n'importe quoi, même si un mail vous promet d'être millionnaire en révélant vos noms et autres coordonnées bancaires !

Pensez en dernier lieu à visiter les options afin de configurer finement vos logiciels.

COURT-CIRCUITER VOTRE FOURNISSEUR D'ACCÈS

Votre fournisseur d'accès (F.A.I.) sait parfaitement qui vous êtes. Il est donc recommandé de se passer d'utiliser ses serveurs pour envoyer et recevoir vos courriers électroniques.

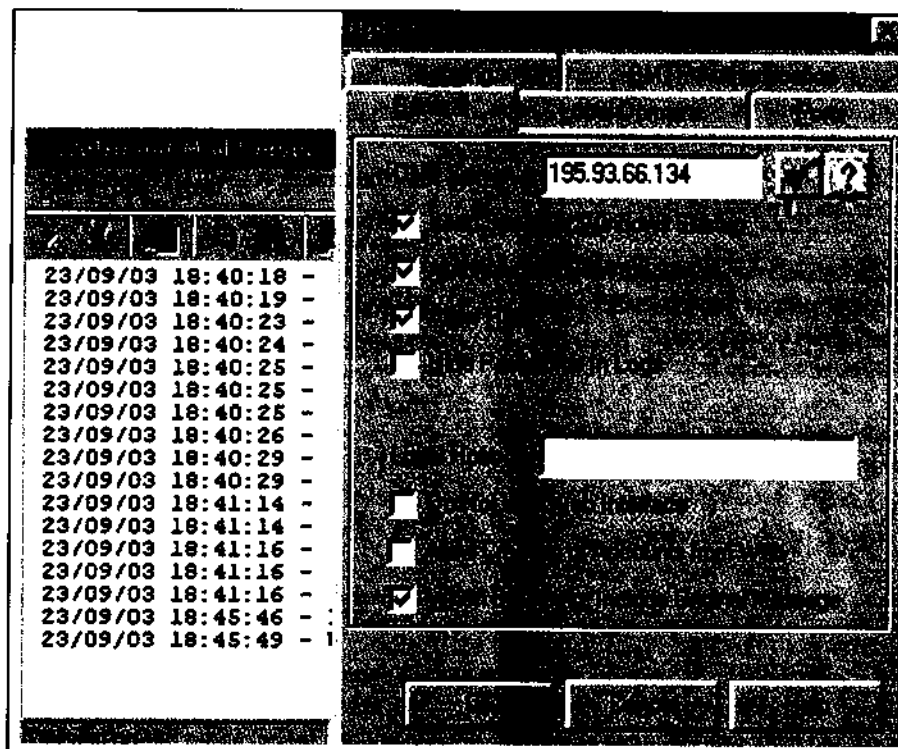
Pour la réception, c'est assez simple : il vous suffit de configurer une adresse email sur un webmail comme Yahoo ou Hotmail (nous en parlerons un peu plus loin), et éventuellement de configurer votre logiciel de messagerie pour récupérer les messages par le protocole POP 3.

Pour l'envoi, vous pouvez aussi utiliser votre logiciel de messagerie. Habituellement, ce dernier est configuré pour utiliser un serveur nommé SMTP de votre fournisseur d'accès internet. Mais il est possible d'en installer un soi-même sur son propre ordinateur, et de cette façon, de court-circuiter le serveur SMTP du FAI. Et si vous avez AOL, cela permet aussi de contourner les limitations imposées par ce fournisseur

d'accès, afin d'utiliser sa propre messagerie avec son propre format. ArgoSoft (<http://www.argosoft.com/applications/mailserver/>) est l'un des meilleurs serveurs SMTP locaux, très simple à manipuler. Nous expliquerons comment installer Post-Cast, un autre serveur SMTP, dans la partie consacrée aux remailers. Lien de téléchargement :

<http://www.argosoft.com/files/apps/agsmail.exe>

Si vous désirez plus d'aide au sujet de ce logiciel, faites un tour sur le site du mail <http://www.arobase.org>. Utilisez leur moteur de recherche intégré puis recherchez l'aide en écrivant "argosoft" dans la fenêtre.



Pour indiquer à votre logiciel de messagerie qu'il doit passer par votre propre serveur SMTP lors de l'envoi des messages, et non par celui de votre FAI, il faut modifier l'entrée " serveur d'envoi " ou " serveur SMTP " dans la configuration de votre compte. Vous devez mettre "127.0.0.1" (adresse IP qui représente toujours votre propre ordinateur). Par exemple, ceux qui ont un compte sur Free devront remplacer "smtp.free.fr" par "127.0.0.1".

DES SERVICES UTILES SUR LES WEBMAILS

Vous pouvez ouvrir une boîte mail gratuite sur n'importe quel site qui propose cette opportunité. Utilisez un pseudonyme de clone virtuel, tel un personnage de dessins animés, et non votre véritable nom. Ne diffusez jamais sur le web tout renseignement vous concernant ! Si une personne, que ce soit par mail, site web ou même par téléphone se prétendant de telle société réputée vous demande vos coordonnées personnelles et/ou bancaires, ou vos identifiants de connexion, refusez tout net.

Parmi les webmails les plus connus, ayant un maximum de fonctionnalité, citons :
<http://www.hotmail.com>
<http://www.yahoo.fr>

L'utilisation de ces sites permet d'avoir un antivirus intégré toujours à jour, ainsi



qu'un anti-spam. Notez que hotmail ferme les comptes mails si ceux-ci n'ont aucune activité pendant 30 jours... Donc si vous recevez trop de publicités, laissez le compte inactif et il sera supprimé automatiquement. Par contre, il faudra penser à prévenir vos "honorables correspondants".

Mais pour le problème du spam, il existe une autre solution. Un site a eu une idée géniale et propose " l'e-mail à durée limitée ". C'est à vous de choisir la durée de vie de la boîte mail que vous allez créer sur : <http://jetable.org>

Pour terminer, voici un moyen basique d'avoir un minimum d'anonymat au niveau des emails. Cela consiste à ouvrir un compte sous un autre nom, sur un site sécurisé qui permet le cryptage de vos messages. Nous vous conseillons :
<http://www.hushmail.com>
<http://www.ziplip.com>

ENVOYER ET RECEVOIR DES EMAIL ANONYMES

L'EMAIL ANONYME, C'EST AUJOURD'HUI LA VERSION MODERNE DE LA BONNE VIEILLE LETTRE ANONYME. VOUS SAVEZ, CELLE QU'ON ÉCRIT EN DÉCOUPANT DES LETTRES DE JOURNAUX, QUE L'ON COLLE SUR DU VIEUX PAPIER, PUIS QUE L'ON DEMANDE À QUELQU'UN DE GLISSER SOUS LA PORTE DU DESTINATAIRE... À PART QUE CETTE FOIS, ON PEUT MÊME RECEVOIR DES RÉPONSES !

Eh bien, c'est presque pareil avec les emails, grâce à des serveurs que l'on appelle...

LES REMAILERS ANONYMES

Un remailer est, en gros, un serveur à qui on envoie un mail, et qui le redirige vers l'adresse souhaitée. Les remailers dont nous allons parler sont ceux dits "anonymes", c'est-à-dire qui ne dévoilent pas l'origine du message (vous) lorsqu'ils le redirigent. Le destinataire ne peut ainsi pas remonter jusqu'à l'auteur du mail. Quand on parle de camoufler " l'origine du message ", on veut parler de l'adresse email source, bien entendu, mais aussi et surtout de votre adresse IP. Cette-ci est en effet contenue dans les en-têtes de chaque message que vous envoyez. Il suffit au destinataire d'afficher la source du message pour visionner ces en-têtes et en déduire votre adresse IP, ainsi que tous les serveurs Internet par lesquels votre message a transité. On peut également savoir quel logiciel de messagerie vous utilisez, et de quelle version il s'agit. Par exemple :


```
Received: from charentes.fr.clara.net (charentes.fr.clara.net
[212.43.194.76])
  by sologne.fr.clara.net (Postfix) with ESMTP id F11861B37E
  for <wanted@dmpfrance.com>; Tue, 2 Dec 2003 00:02:48 +0100
(CET)
Received: from gw-smtp.canl.nc (gw-smtp.net-outremer.nc
[202.171.64.2])
  by charentes.fr.clara.net (Postfix) with ESMTP id 0C2E0596DC
  for <wanted@dmpfrance.com>; Tue, 2 Dec 2003 00:02:48 +0100
(CET)
Received: from mail3.canl.nc ([202.87.159.2] helo=mail1.canl.nc)
  by gw-smtp.canl.nc with esmtp (Exim 4.14)
  id 1AQx40-0006fZ-4a
  for wanted@dmpfrance.com; Tue, 02 Dec 2003 10:02:44 +1100
Received: from 203-117-65-122.noc-poe1.net-outremer.nc
([203.117.65.122] helo=canl.nc)
  by mail1.canl.nc with esmtp (Exim 4.24)
  id 1AQx4A-00029O-50
  for wanted@dmpfrance.com; Tue, 02 Dec 2003 10:02:54 +1100
Date: Tue, 02 Dec 2003 10:05:04 +1100
From: Superman <pierre@serveur.canl.nc>
User-Agent: Mozilla/5.0 (Macintosh; U; PPC; fr-FR; rv:0.9.4)
Gecko/20011130 Netscape6/6.2.1
Accept-Language: fr-fr
To: wanted@dmpfrance.com
```

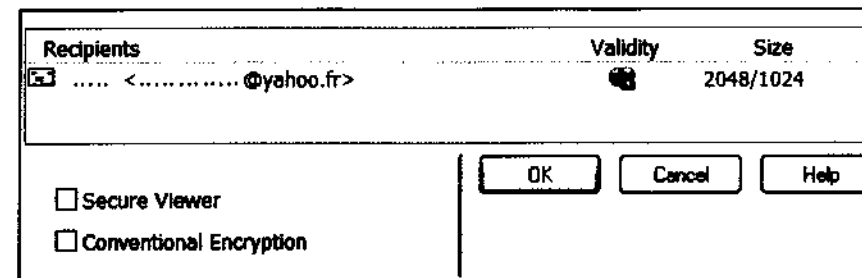
On voit que l'adresse IP de l'expéditeur était 203.117.65.122, et que le message a été envoyé avec Mozilla en langue française.

Intéressé pour rendre intraquables vos envois de messages ? Alors continuez à lire, car si le principe est simple, l'exécution l'est un peu moins, et il y a certaines techniques à maîtriser pour atteindre l'anonymat (presque) parfait.

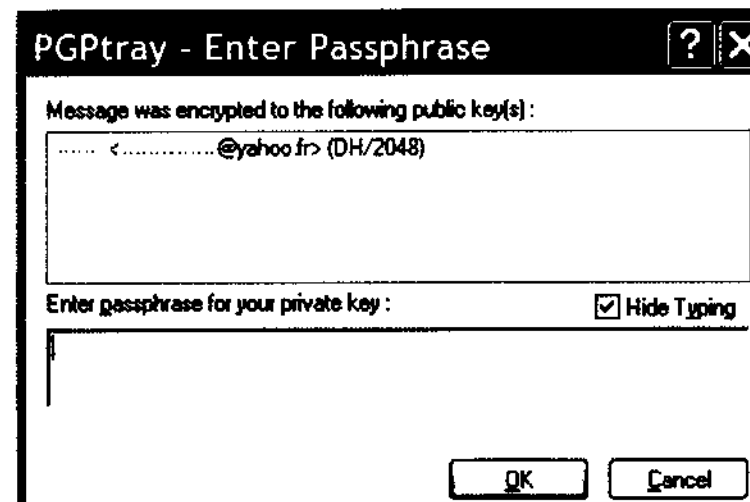
D'abord, il va falloir installer PGP si vous ne l'avez pas déjà fait. En effet, la plupart des remailers est configurée pour n'accepter que des messages encryptés pour plus de confidentialité (on y reviendra plus loin). Vous pouvez trouver les adresses où télécharger les dernières versions gratuites de PGP sur :

<http://www.pgpi.org/products/pgp/versions/freeware/>.

Lors de l'installation, vous créez une paire clé publique/clé privée : en résumé, la clé publique est celle que vous donnez à vos contacts pour qu'ils encryptent des messages, que vous seul serez capable de décrypter, à l'aide de votre clé privée. Prenons un petit exemple pour être sûr que vous maîtrisiez bien la bête : ouvrez le bloc-notes et tapez un court texte, puis copiez-le par Ctrl-A/Ctrl-C. Cliquez avec le bouton droit



sur la petite icône de PGP, et sélectionnez Clipboard/Encrypt. Dans la liste "Recipients", vous devez indiquer les destinataires du message, en l'occurrence vous, puisqu'il ne s'agit que d'un test, puis cliquez sur OK.



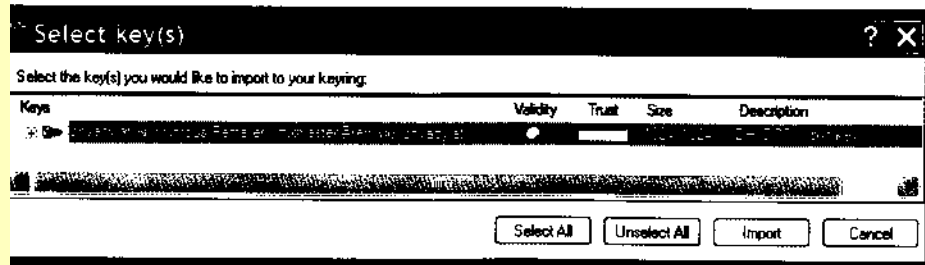
Le message encrypté (grâce à votre clé publique) est alors copié dans le presse-papier, vous pouvez le visualiser dans le bloc-notes, ça doit ressembler à ça :

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

yANQR1DBwU4DA+05PLAbrXIQB/0Q1/bG4mEfiAi4mg/HkOuf8CrgmdGrYPnsB2N3
o19w4j7p9Xx1ODOP100PmDD9LMA+nwVUDuXG/u04wyXgyfnVHo17yaiJNFVAUz/+
Jah+9WRshaL6RwWyD6W0FqrQ3ezynPI60ts00Z4bkLUL1Tq+PI/rLHF0r2z37dwY
-----END PGP MESSAGE-----
```

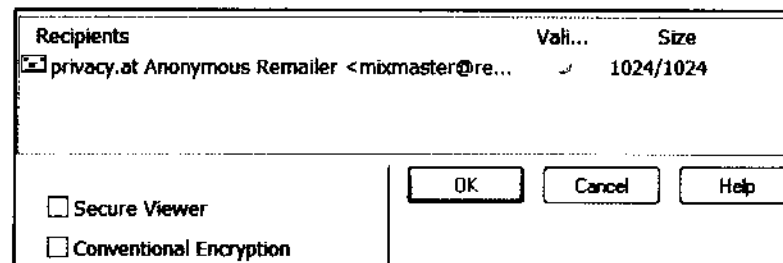
Pour le décrypter, un nouveau clic droit sur l'icône de PGP, et cette fois-ci, choisissez Clipboard / Decrypt and Verify.

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia) http://www.pdfmail.com



Vous devrez encore rentrer la "passphrase" correspondant à votre clé privée : c'est une phrase qu'on vous a demandée lors de la création de votre paire de clés, et qu'il ne faut jamais oublier sous peine de ne plus pouvoir décrypter ses messages (il est également conseillé de ne jamais l'écrire nulle part, et de ne pas prendre des phrases trop classiques, comme une citation).

Bien, maintenant nous allons utiliser un remailer pour envoyer un mail crypté anonyme. Le principe est le suivant : vous envoyez le mail crypté au remailer, qui le décrypte et l'envoie en clair au destinataire final. Pour cela, il vous faut bien sûr la clé publique du remailer. Nous allons commencer par faire des expériences avec le remailer "austria" (mixmaster@remitter.privacy.at), mais s'il ne marchait pas au moment où vous lisez ce guide, voyez un peu plus loin pour d'autres remailers. Pour demander une clé publique à un remailer, il faut lui envoyer un email dont le sujet contient simplement "remitter-key" (sans les guillemets). La réponse arrive généralement dans la minute qui suit, et contient plusieurs clés, en principe une clé Mix-



master et deux clés PGP, de la forme :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mixmaster 2.9.0 (OpenPGP module)

mQCNAziXaLgAAAEAAOTgQxgxJ4zdkZeY3db4vHK4qZYCN+wh+A31848WBNC+1/9S
Ca56PnaE/yTA3P5AW5Da4g96KoLMYPQQwURPzgIX1yCK6NIDqE/7Y3AfZPcPyBd1
ikG8aaWzaNZTBV/EyEn0P31VrpgTS9oMa5SIDabEDakVv3sj38LCjIDvaPU1AAID
-----END PGP PUBLIC KEY BLOCK-----
```

Pour l'instant intéressons-nous uniquement aux clés PGP. Les deux clés correspondent aux protocoles RSA (la plus courte) et DH/DSS (la plus longue). Il vous suffit d'une seule, c'est généralement la DH/DSS qui est la plus utilisée, mais vous ne prendrez pas de très grands risques en utilisant la RSA (pour plus d'informations sur les différences entre les deux protocoles, visitez <http://www.scramdisk.clara.net/pgp-faq.html>). Copiez donc le bloc correspondant à la clé (en incluant "-----BEGIN PGP

PUBLIC KEY BLOCK-----" et "-----END PGP PUBLIC KEY BLOCK-----"), puis cliquez sur l'icône PGP, encore sur Clipboard / Decrypt and Verify.

Vous devez voir la clé du remailer, il ne reste plus qu'à cliquer sur "Import" pour pouvoir l'utiliser. Maintenant, allez dans votre client mail (ou dans le bloc-note), et tapez votre message. Cet email doit avoir un format spécial, de la forme :

```
::  
Anon-To: Hackademy <hackademy@dmpfrance.com>
```

```
##  
Subject: Bonjour !
```

Ceci est un email anonyme...

Bien sûr, le champ "Anon-To" indique le destinataire du mail, "Subject" le sujet, et ensuite on met le texte du mail proprement dit. Il faut maintenant crypter tout ça : copiez le texte, puis encryptez-le à l'aide de la clé publique du remailer. Dans "Recipients", vous devez donc mettre le remailer que vous allez utiliser :

Ce document a été fabriqué par PDFmail (Copyright RTE Multimedia)
<http://www.pdfmail.com>

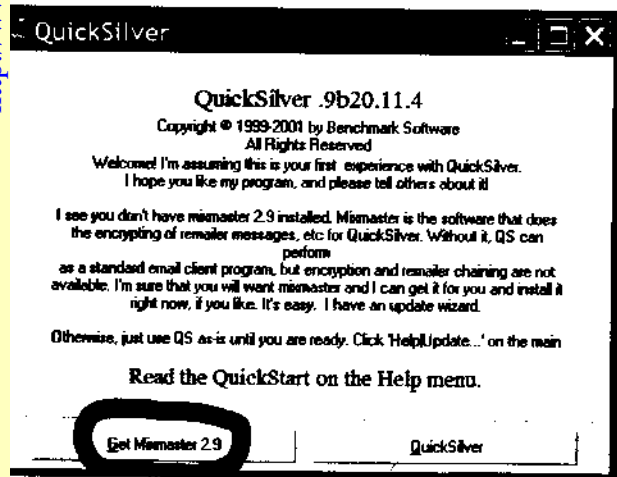
Cliquez sur OK, et copiez le contenu du presse-papier dans votre client mail. Il reste à indiquer qu'on a encrypté le message à l'aide de PGP, ce qui se fait en rajoutant un petit en-tête, de manière à ce que votre message, au final, ressemble à :

```

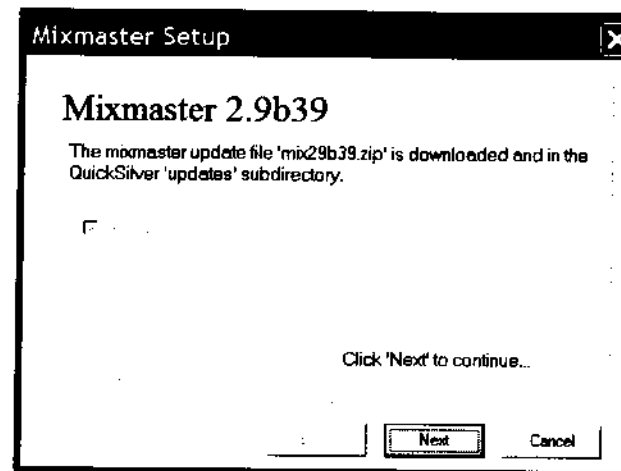
::
Encrypted: PGP

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

qANQR1DBwE4DTpBM/M97kj4QA/4qUCm4FNYbDMmq4fjVu6PEH0PYuCWZPVU53Ws
npqXR+BZSvdaVl7RXb11lpFEdNQtSoiWxdjjwi+fXzx61Ko0r8TQv1RMymzHOSO
5ofH9tundoy9pXN3aurR9U9wVv4BpiSF9djet3835in6U1KlXK9VJQ5iImAS3UGV
-----END PGP MESSAGE-----
    
```



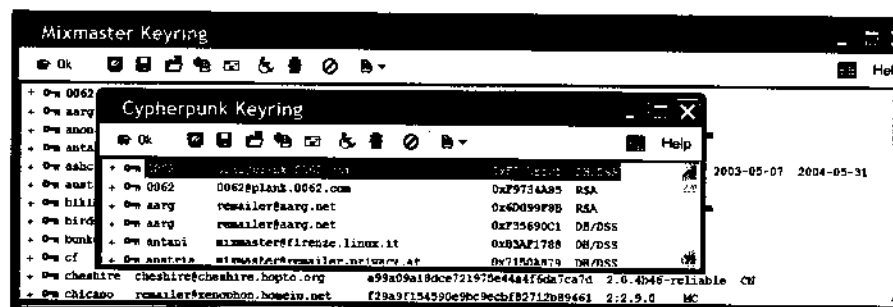
ous enverrez cet email à mixmaster@remailer.privacy.at, sans rien mettre dans le sujet. Il est conseillé de vérifier d'abord que tout fonctionne bien en s'envoyant un mail à soi-même. Attention ! La plupart des remailers ont un certain "temps de itence", c'est-à-dire que votre email ne sera pas envoyé immédiatement à son des-



tinataire. Il y a plusieurs raisons à cela :

- déjà, un remailer peut se retrouver particulièrement chargé, et votre mail devra donc attendre avant d'être pris en compte.
- d'autre part, introduire un délai fait partie du processus d'anonymat. Savoir à quelle heure exactement un mail a été envoyé peut en effet permettre de démasquer son auteur.
- pour encore plus de sécurité, les mails ne sont pas envoyés dans l'ordre dans lequel ils sont reçus. Cela permet d'éviter que quelqu'un puisse retracer un email en analysant le trafic (ce n'est pas quelque chose de facile à faire, mais c'est possible).

Soyez donc patient en attendant votre email. Il devrait finir par arriver. Pour savoir plus précisément combien de temps on peut s'attendre à attendre (par exemple une



vingtaine de minutes pour le remailer austria), il existe des pages web de statistiques, qui sont également une bonne source d'adresses de remailers. Vous en avez par exemple sur <http://mixmaster.shinn.net/stats/remailer-list.html> et sur

<http://anon.efga.org/Remailers/TypeList>. Regardez dans la liste à la fin, il y a des tats du type :

emailer	email address	history
atency	uptime	
ustria	mixmaster@remailer.privacy.at	+*****
:23:34	99.49%	

est conseillé de choisir un remailer ayant un uptime (pourcentage de temps de fonctionnement) aussi haut que possible, et un temps de latence ("latency") aussi bas ue possible (si vous voulez que votre email arrive vite bien sûr, ce qui n'est pas forcément le cas).

ous pouvez également trouver des pages web contenant les clés publiques des emailers, mais il est plus sûr de les demander directement au remailer par la com-



vande remailer-key. D'autres commandes utiles (à mettre dans le sujet d'un mail) ont remailer-conf (pour savoir comment est configuré le serveur), remailer-stats pour voir des stats sur le nombre d'emails traités), et remailer-help (si vous êtes perdu). La configuration d'un remailer est particulièrement importante. Elle est synthétisée par une ligne du type "cpunk mix pgp pgponly reppg remix latent hash cut ist ek ekx esub inft50 rhop20 reord klen1024". Les options les plus importantes our ce qui nous a intéressé jusqu'à présent sont "cpunk" (Cypherpunk Remailer, est-à-dire acceptant les messages cryptés) et "pgp" (supporte l'encryption par PGP).

CHAÎNER LES REMAILERS

Avec tout ça, vous devriez être capables d'envoyer de jolis mails anonymes. Mais si vous êtes vraiment paranos, vous avez peut-être entendu parler de rumeurs selon lesquelles certains remailers seraient maintenus par le FBI ou la CIA. Certes, ce ne sont que des rumeurs, mais rien ne dit qu'elles ne sont pas fondées (oui, on aime entretenir votre paranoïa). Même si les remailers anonymes ne gardent officiellement pas de logs et ne vérifient pas le contenu de vos emails, vous ne pouvez que vous fier à leur bonne foi pour la protection de votre anonymat : il y a toujours le risque que l'on remonte jusqu'à vous puisque le remailer sait qui a envoyé le mail, et qu'on espionne vos communications puisque le remailer peut les décrypter.

Pour pallier ce problème, la solution consiste à "chaîner" les remailers, c'est-à-dire à faire se balader votre mail entre plusieurs remailers avant de le délivrer à son destinataire. Par exemple, supposons que vous vouliez utiliser une chaîne R1 -> R2 -> D, où R1 et R2 sont des remailers et D la destination. Vous commencez par créer un email comme si vous utilisiez juste le remailer R2. Vous rajoutez alors l'en-tête suivant :

```
::
Anon-To: adresse_R2
```

puis vous encryptez cet email pour l'envoyer à R1 (donc avec la clé publique de R1). Lorsque R1 le reçoit, il le décrypte (mais seulement la première "couche" de cryptage) et s'aperçoit qu'il doit l'envoyer à R2. R2, lui, décrypte la seconde couche et l'envoie à D. Intérêt : seul R1 connaît l'origine, et seul R2 connaît le contenu et le destinataire (ça, vous n'y pouvez pas grand chose, puisque le message doit être envoyé en clair au destinataire). Evidemment, vous pouvez introduire d'autres remailers au milieu, qui eux ne connaîtront ni l'origine, ni le destinataire, ni le contenu du mail (d'où l'intérêt de l'encryption systématique). Donc tant pis pour le FBI : espionner le trafic ne sert plus à rien.

Notez que les remailers qui ont le mot-clé "middle" dans leur configuration sont configurés pour automatiquement relayer votre email à au moins un autre remailer avant livraison, si vous n'avez pas spécifié de chaîne vous-mêmes.

LE MAÎTRE DU MIX

Et ce n'est pas fini ! Certains ont trouvé que l'anonymat n'était pas suffisant avec un tel système, ce qui a donné naissance à un autre type d'encryption pour les remailers, appelé "Mixmaster". Les remailers compatibles avec ce protocole sont appelés

remailers de type 2 (alors que les remailers "Cypherpunk" sont de type 1), et sont caractérisés par la présence du mot-clé "mix" dans leur configuration (la plupart des remailers de type 2 sont également compatibles avec le cryptage de type 1).

Mixmaster est spécialement conçu pour renforcer la sécurité dans les chaînes de remailers : l'encryption est basée sur RSA et le triple DES, et les messages ont tous la même taille (28.1 Ko) et sont réordonnés, de manière à empêcher de les suivre par l'analyse du trafic. Par contre, l'inconvénient est qu'il faut utiliser un programme spécial pour construire ses mails anonymes. Les deux programmes les plus utilisés sont QuickSilver (<http://quicksilver.skuz.net/>, la dernière version au moment d'écrire cet article se trouve sur <ftp://skuz.net/pub/quicksilver/QS.9b20.11.4.exe>) et Jack B. Nymble 2 (<http://www.bigfoot.com/~potatoware/jbn2/index.html>).

Comme il faut bien faire un choix, c'est QuickSilver que nous allons vous apprendre à utiliser ici. Jack B. Nymble 2 ne fonctionnait pas bien sur notre machine tournant sous XP. Lors de l'installation, QuickSilver commence par vous demander votre adresse email et votre serveur SMTP habituel, donnez-lui ici de vraies infos (au moins pour le serveur), sinon vous risquez d'avoir des problèmes pour envoyer vos mails. Au lancement, il détecte que nous n'avons pas encore installé la librairie de cryptage Mixmaster et nous propose de la télécharger. Pas d'hésitation, cliquons sur "Get Mixmaster 2.9".

Il se connecte alors sur le FTP de QuickSilver et nous propose de télécharger un des modules : celui qui nous intéresse se nomme "Mix29b39.zip", sélectionnez-le dans la liste et cliquez sur "Next". Après le téléchargement, cliquez sur "Run Setup". Une confirmation de l'installation de Mixmaster s'affiche.

Cliquez sur "Next", choisissez le répertoire d'installation de Mixmaster, "Next", "Install", "OK"... on y est presque, il reste à accumuler des données aléatoires, ce qui se fait en raçant des traits à la souris jusqu'à ce que le compteur indique 100%. Ensuite, "Exit", puis "OK", et QuickSilver se lance enfin ! Vous pouvez désactiver la fenêtre "For beta testers only" qui se lance par défaut au démarrage.

Il ne reste plus qu'à configurer la bestiole, en commençant par lui rentrer quelques infos sur les remailers. Allez dans Tools / Remailers. Cochez les 4 cases devant "mlist.txt", "publist.mix", "rlist.txt" et "pubring.asc" puis cliquez sur Update. Le programme télécharge automatiquement toutes les infos nécessaires. Cliquez sur OK : vous voyez maintenant deux fenêtres, "Mixmaster Keyring" et "Cypherpunk Keyring", contenant les clés Mixmaster et PGP des différents remailers. Toutes les clés sont téléchargées automatiquement, c'est bien, mais il est plus prudent de s'assurer que ce sont bien les dernières en les mettant à jour manuellement. Cette technique permet aussi d'utiliser QuickSilver, même si les sites avec les clés disparaissent. Pour cela, utilisez la méthode vue plus haut pour demander leur clé aux remailers que vous souhaitez utiliser. Pour chacun d'eux, sélectionnez tout le contenu du mail conte-

nant les clés et copiez-le dans le presse-papier. Cliquez alors, avec le bouton droit, dans la fenêtre "Mixmaster Keyring", et choisissez "Import...", et enfin cliquez sur "Clipboard". Si le message "NO NEW KEYS" apparaît, cela signifie que vos clés sont à jour, tout va bien. Sinon, vous importerez la nouvelle clé qui apparaîtra dans la liste.

Il est temps maintenant d'envoyer notre premier mail mixmaster : dans le menu "File", choisissez "New" puis "Message". Le champ "Host" doit contenir votre serveur SMTP, le champ "From" est presque inutile puisque le remailer le changera, le champ "To" contient bien sûr la destination, et enfin le champ "Chain" indique quels remailers vous voulez utiliser (par exemple "austria.hastio" en spécifiant les noms, ou "*", "*", "*" pour une chaîne de trois remailers aléatoires, ou "*.austria" pour choisir un premier remailer aléatoirement et spécifier le second comme austria).

Si vous avez mis à jour les clés manuellement, vous préférerez désactiver l'option "Update on Send" du menu "Tools", qui permet de re-télécharger toutes les clés juste avant d'envoyer un mail, pour être sûr d'être à jour. Vous pouvez maintenant cliquer sur "Send". Si le mail ne veut pas partir et que votre serveur mail est correctement entré, c'est peut-être que le serveur de votre fournisseur d'accès empêche le relais de mails. Dans ce cas-là, lisez l'encadré "Installer son propre serveur SMTP".

UN COMPTE EMAIL ANONYME

Envoyer des mails anonymes, c'est bien, mais que dites-vous d'en recevoir aussi ? La tâche est un peu plus compliquée, car vous devez récupérer vos emails, ce qui implique de se dévoiler.

Il existe bien des services de webmail "sécurisés" comme Hushmail (www.hushmail.com), mais vous pouvez toujours être identifié... Le meilleur moyen de recevoir des mails anonymement est de créer un compte nym, ce que nous allons faire pas à pas dans la suite.

Comme pour les remailers Cypherpunk, vous allez avoir besoin de PGP, alors s'il n'est pas encore installé, dépêchez-vous ! Le serveur nym.alias.net est le plus populaire, mais pas le plus rapide d'après mes essais : deux autres serveurs nym sont redneck.gacracker.org (celui que nous allons utiliser ici) et nym.xganon.com. Commencez par envoyer un email sans sujet ni texte à remailer-key@redneck.gacracker.org. Vous devriez recevoir (bientôt avec un peu de chance, soyez patient...) la clé PGP du serveur, que vous importerez dans vos clés PGP comme auparavant. Ensuite, envoyez un mail à list@redneck.gacracker.org : vous aurez en réponse la liste de tous les alias déjà utilisés sur ce serveur, de façon à ce que vous n'en choisissiez pas un qui existe déjà.

En attendant la réponse, nous allons créer notre "reply block", c'est-à-dire le bloc qui va indiquer au serveur nym comment nous envoyer les mails qui nous sont destinés. Pour faire simple, je vais prendre ici l'exemple où vous utilisez simplement le remailer "austria" entre vous et le serveur nym. Commencez par taper les instructions pour diriger les emails vers votre vraie adresse :

```

:
Anon-To: hackademy@dmpfrance.com
Encrypt-Key: piratownz
    
```

Le champ "Encrypt-Key" est facultatif, mais sert de sécurité supplémentaire : il s'agit

INSTALLER SON PROPRE SERVEUR SMTP

Parfois, le serveur de mail de votre fournisseur d'accès est configuré pour vous empêcher certaines fonctions : par exemple il peut ne pas accepter de relayer des emails (fonction utilisée par QuickSilver), ou ne pas fonctionner avec un programme comme Ghost Mail. Dans un tel cas, il peut être utile d'installer soi-même un petit serveur SMTP sur sa machine afin de pouvoir envoyer des emails sans passer par le serveur de son provider. Il existe de nombreux serveurs, et notamment un gratuit sous Windows, s'appelle Postcast Server et peut se télécharger sur :

Après l'installation, qui ne pose pas de difficulté particulière, lancez le programme, qui affiche le "Setup Wizard". Cliquez sur "Next", puis cochez (en tout cas je vous le conseille) la case "Allow access only from users with these IP addresses", et n'autorisez que votre propre IP (127.0.0.1) à envoyer des mails (sinon vous risquez de voir quelqu'un envoyer des mails à partir de votre ordinateur, ce qui pourrait vous causer des ennuis). Cliquez sur "Next", et choisissez d'envoyer les messages "Immediately". Cliquez enfin trois fois sur "Next", puis sur "Finish".

Pour utiliser votre serveur de mail tout neuf, vous devez spécifier le serveur smtp "127.0.0.1". Par exemple, dans QuickSilver, la ligne "Host" doit être : Host: 127.0.0.1. Si vous remarquez que vos mails ne partent pas, c'est peut-être que votre fournisseur bloque le port 25 en sortie (ce que de plus en plus font, pour bloquer les spammers). Dans ce cas, il n'existe malheureusement que peu de recours : utiliser une autre machine à laquelle vous avez accès pour relayer les messages, ou employer par exemple le service "Mail reflector" de no-ip.com, qui coûte quand même 10 \$ / an...

MESSAGERIE INSTANTANÉE : MSN, ICQ, AIM, YAHOO MESSENGER...

À PROPOS DE MSN MESSENGER ET DE SES CONFRÈRES... COMMENT GARANTIR SON ANONYMAT, S'AFFRANCHIR DE LA PUBLICITÉ ET DES LOGICIELS ESPIONS !

ÉLIMINER LA PUB ET LE FLICAGE

Il existe une bonne part de rumeurs dans les allégations sur les fonctions supposées d'espionnage de ces logiciels. Mais dans le doute, mieux vaut se méfier !

Amis lecteurs, les utilisateurs de Microsoft Messenger déplorent la présence de publicité abusive provenant de Microsoft. Nous vous proposons de réduire à néant l'invasion publicitaire sur votre PC. Cliquez sur "Démarrer>Exécuter", entrez "msconfig" puis cliquez sur "OK". L'utilitaire de configuration système apparaît. Cliquez sur l'onglet "Démarrage" puis décochez "Load QM". Par contre, à vous de voir si vous désirez que Messenger démarre en même temps que Windows. Dans le cas contraire vous pouvez décocher la case "MSMSG". Cliquez sur "appliquer".

Une fois que votre ordinateur aura redémarré, la nouvelle configuration de MSN Messenger sera prise en compte. Toutefois je vous invite à désinstaller ce programme qui offre peut-être à son éditeur une opportunité pour vous espionner, et une porte d'entrée aux pirates. En effet, les logiciels de Microsoft sont beaucoup plus reliés au reste du système d'exploitation que ceux des éditeurs indépendants, et sont donc plus susceptibles d'ouvrir des trous de sécurité.

La messagerie instantanée de ICQ apporte nombreuses fonctionnalités, mais elle aussi est connue pour inclure quelques espions, afin de tracer votre comportement de consommateur et de vous cibler lors de la parution de bannières publicitaires. L'équipe du site <http://www.zebulon.fr> fournit cette solution : lancez le programme

"regedit" afin d'éditer la base de registre, allez dans HKEY_CURRENT_USER/Software/Mirabilis/ICQ/Defaultprefs, et transformez la valeur de la clé AutoUpdate de "yes" à "no". Les infos ne devraient plus remonter jusqu'aux serveurs de la société Mirabilis.

Même le messenger d'AOL, dénommé AIM, pourrait rapporter des informations commerciales sur vos habitudes de surf. D'ailleurs, il existe sur le Net un programme en anglais efficace, dénommé DeadAIM, qui permet de bannir la publicité d'AIM et de le configurer plus finement. Vous pouvez le télécharger à l'adresse suivante :

<http://www.jdennis.net/DeadAIM/about.php>
Sinon, vous pouvez le trouver en le recherchant, par le biais d'un moteur de recherche tel google.fr.

L'ANONYMAT

DES MULTI-MESSENGERS

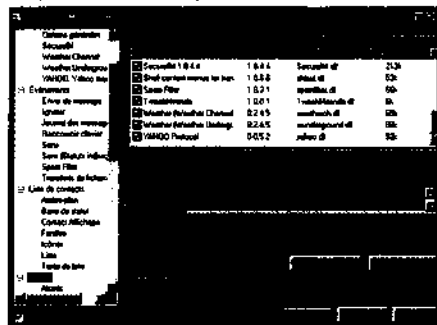
Autant télécharger un programme libre, gratuit et sans spyware, plutôt que ces logiciels hautement commerciaux et qui ont tous été sujets, dans le passé, à des failles de sécurité critiques. Qui plus est, un logiciel libre respectera beaucoup plus votre vie privée. L'idéal est d'installer un multi-messengers, c'est-à-dire un logiciel qui offre en un seul programme une connectivité sur de multiples réseaux :

- AIM
- Jabber
- ICQ
- IRC
- Yahoo

- Horloge atomique
- MSN
- RSS
- et même Gadu-gadu (réseau polonais) !

Vous pouvez utiliser, par exemple, le très bon logiciel Miranda, disponible en téléchargement à l'adresse :

<http://www.nortiq.com/miranda>

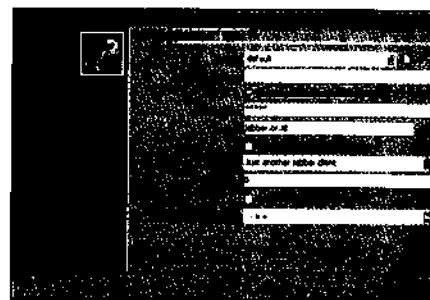


Visitez en priorité les plug-ins et la page des protocoles (AIM, Yahoo, Icq, RSS, SMTP, Jabber, Gadu-Gadu, MSN, etc.) ainsi que celle de la sécurité (connexion sécurisée, anti-spams, cryptage). Les skins et autres amusements attendront ;-)

Il existe des multimessengers sous serveur Jabber, disponible sur le site <http://www.jabber.org>. Cliquez sur "download a client". Pour ce qui concerne "les Jabber", nous vous préconisons JAJC et PSI qui fonctionnent sans utiliser une DLL du navigateur Internet Explorer. Bannissez les autres.

Ensuite, vous choisirez un serveur Jabber et c'est sous son adresse IP que l'on pourra vous identifier... et non sous votre propre adresse ! Voilà un bon point pour rester anonyme.

De plus, vous pourrez configurer les



multimessengers avec un serveur proxy qui vous dissimulera encore mieux. Concernant Miranda, vous pouvez le faire tourner sous un ou plusieurs de

ces protocoles, et même le dissimuler sous un serveur jabber. L'anonymat à l'état pur.

Gaim, un autre multimessenger, n'est pas mal non plus... quoique lourd. À télécharger sur <http://gaim.sourceforge.net>. Un dernier programme de ce type, léger et rapide, avec moins d'options que Miranda mais très facile à utiliser : <http://www.easymessage.net>. Miranda est toutefois notre choucho : il est léger, stable et multifonctions.

LES LOGICIELS "PEER TO PEER" DE PARTAGE DE FICHIERS

LE PEER TO PEER, OU P2P, EST UN SUJET BRÛLANT. CONSACRÉS AUX ÉCHANGES DE FICHIERS BIEN SOUVENT ILLÉGAUX, CES RÉSEAUX SONT EXTRÊMEMENT SURVEILLÉS, ET CONSTITUENT DES LIEUX PRIVILÉGIÉS DE PROPAGATION DES VIRUS. S'Y CONNECTER EN TOUT ANONYMAT N'EST CEPENDANT PAS IMPOSSIBLE.

Avec les actions récentes de la RIAA contre des usagers de Kazaa, sans compter les lettres qu'ont pu recevoir certains abonnés français suite à des plaintes d'associations de lutte contre le piratage, et la menace Retspan qui plane toujours, l'anonymat sur les réseaux P2P revêt beaucoup d'attraits. Non pas pour dissimuler vos activités illicites (qui n'existent pas de toute manière), mais surtout pour, au moins, avoir enfin un peu de paix. L'anonymat sur les réseaux peer 2 peer est cependant un challenge compliqué, car pour se cacher, il faut introduire des intermédiaires (comme les emailers pour le mail), ce qui ralentit forcément le débit... Mais commençons par le début : quel logiciel utiliser ?

LES DANGERS DU P2P

Kazaa est le programme de P2P le plus espionné, et peut-être le plus espionnable vu la présence de nombreux trous de sécurité. Ce n'est pas pour rien que les majors attrapent des internautes échangeant des fichiers musicaux qui utilisent ce programme. Il contient des spywares et a besoin d'Internet Explorer pour fonctionner. Même sa version dite Lite, où les spywares sont éliminés, a besoin du navigateur de Microsoft...

Aux USA, il est fréquent que les majors révèlent les noms d'utilisateurs qui tourmentent nous avec Kazaa. Mais bien sûr, il n'y a pas que Kazaa qui rentre dans cette catégorie des logiciels P2P à spywares, ou qui ont besoin d'Internet Explorer pour tourner :

- BearShare
- LimeWire
- OverNet
- Kazaa Lite
- Edonkey

- Blubster
- Piolet
- Emule, qui est open source, a besoin de I.E. lui aussi (!)

Note : le site de WinMX signale que le logiciel a besoin d'IE pour fonctionner, mais après que nous l'ayons testé, nous pouvons vous affirmer qu'il tourne sans le navigateur de Microsoft.

De plus, ces logiciels présentent régulièrement des failles de sécurité révélées par leurs utilisateurs. Il est important de les mettre à jour régulièrement.

Sachez cependant que le pire danger vient du principe même du peer 2 peer, qui est de connecter directement deux ordinateurs appartenant chacun à un particulier. En effet, pour pouvoir communiquer, chacun des deux ordinateurs connectés doit connaître l'adresse IP de l'autre. Sur un réseau Peer 2 Peer classique, il est donc très simple d'obtenir l'adresse IP (et donc le nom et prénom, dans le cas des forces de l'ordre) de tout utilisateur.

QUELLES SONT LES SOLUTIONS ?

Nous allons résumer ici les mesures que vous pouvez prendre pour vous protéger et vous assurer ainsi d'un minimum d'anonymat et de sécurité sur ces réseaux. Les points les plus importants seront détaillés par la suite.

- choisir un programme réellement fiable, tel Filetopia qui propose un cryptage, voire WinMX ou FreeNet pour les plus aguerris (lire notre comparatif ci-après). Visitez toujours les options des programmes que vous installez. Cela vous permettra toujours de mieux vous protéger que par la configuration par défaut.
- changer le port attribué d'origine... si possible, car de nombreux programmes ne pourront plus fonctionner, le port étant imposé par le ou les serveurs.
- éviter les programmes qui passent par un serveur (relais) central car celui-ci peut être piraté afin de mieux vous tracer. De plus, le propriétaire du serveur peut fournir les logs de connexion à qui veut... et qui paie !
- utiliser un serveur proxy d'anonymat, de préférence basé dans les pays de l'Est et de type socks 5 sur le port 1080. Si votre programme de P2P ne le permet pas, vous pouvez essayer de le "socksifier" avec SocksCap pour qu'il puisse, malgré tout, passer par un proxy (lire l'article sur les proxies pour plus de détails).
- bien entendu, ne pas laisser son disque dur complet en libre partage, mais créer simplement un dossier que vous mettrez en lecture seule via les "propriétés".
- créer un pseudo et une boîte mail sur un webmail comme Hotmail.com ou Voila.fr, voire une boîte valable quelques jours sur <http://jetable.org>.

- installer un antivirus et un firewall (Antivir + Kério feront très bien l'affaire). Ces logiciels efficaces vous aideront à sécuriser votre PC. Tous les fichiers que vous y téléchargerez devront être scannés par votre antivirus.

L'idéal serait de faire du P2P avec un autre PC que celui qui contient des données importantes, ou bien avec un autre disque dur. Ceux qui font de l'échange de fichiers sur leur PC au travail se reconnaîtront... Qu'ils sachent qu'ils peuvent être tracés, que ce soit par l'administrateur réseau, par des sociétés privées travaillant pour les majors de la musique, ou... par les pirates à l'affût de données d'entreprise intéressantes ! Sachez qu'un scanner comme Nessus (<http://www.nessus.org>) est capable de détecter à distance qu'un programme P2P tourne sur votre PC.

N'oubliez pas également que votre fournisseur d'accès internet peut être sollicité par les services judiciaires, et leur donnera accès aux journaux d'historiques de connexions vous concernant. Le mieux est donc de s'abstenir de tout comportement illégal et de bien contrôler tout ce que l'on télécharge, car il peut y avoir des virus cachés et autres troyens.

Les bons vieux conseils concernant les emails sont toujours valables sur les réseaux peer to peer : n'accordez pas votre confiance à des inconnus, ne donnez sous aucun prétexte vos informations personnelles, même (et surtout) si l'on vous fait du baratin... On ne s'imagine pas le nombre d'internautes mâles qui peuvent cliquer sans scanner auparavant avec leur antivirus sur des fichiers d'images à connotation érotique. D'ailleurs, les dames ne sont pas en reste si on leur propose des fichiers avec des noms de fleurs, de bébés ou de petits chats ! Certains virus volent même des vrais fichiers de sociétés et/ou de particuliers, puis les auto-voient en s'incluant dedans. Et hop, un clic imprudent de l'une ou de l'autre sur un fichier infesté et vos données personnelles sont étalées sur le Net...

Sachez que le P2P, les mails et l'IRC sont d'excellents moyens de transport de ces saletés. Donc, si vous désirez préserver votre sécurité et votre anonymat, deux précautions valent mieux qu'une !

UTILISATION D'UN LOGICIEL DÉDIÉ À L'ANONYMAT

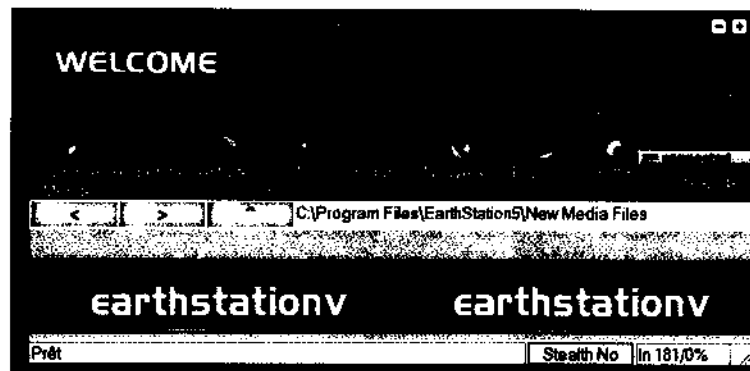
Il existe quelques projets de Peer 2 Peer spécifiquement dédiés à l'anonymat. Nous les avons testé pour vous.

Le projet Freenet (<http://www.freenetproject.org/>) continue tranquillement son développement, et pourrait s'avérer une solution viable à terme. Par contre son objectif est clairement l'anonymat avant la performance, ce qui le rend peu pratique pour les gros fichiers, et se traduit aussi par des fonctions de recherche très basiques. Le prin-

cipe est que les données partagées sont réparties, encryptées, entre les différentes personnes connectées au réseau. Ces dernières ne savent pas elles-mêmes ce qu'elles mettent à disposition sur leur disque ! Lorsqu'un téléchargement a lieu, les données sont transférées par une multitude de personnes connectées au réseau, qui servent d'intermédiaires, avant d'arriver finalement au véritable demandeur.

Filetopia (www.filetopia.org), est un autre réseau orienté vers l'anonymat, avec encryption des données. Par contre, pour cacher son adresse IP, il faut passer par des "bouncers", qui sont l'équivalent de proxies : non seulement il vous faudra vous-mêmes dénicher un bouncer, mais en plus, à moins de connaître personnellement la personne qui le fait tourner, comment pouvez-vous être sûr qu'elle ne va pas justement s'amuser à vous espionner ?

Ce n'est décidément pas ce qu'il y a de mieux, alors voyons ce qu'Earth Station 5 (www.earthstation5.com) peut nous proposer : encryption (des transferts et sur disque grâce à pgpDisk), utilisation de l'UDP au lieu du TCP/IP, mouais... Ohoh, "serveur proxy", qu'ils annoncent, en un seul clic de souris ! Tout alléché, nous installons la bête, malgré un mauvais pressentiment dû au look horrible de leur page web. Pressentiment qui se confirme en voyant à quoi ressemble le programme. Après avoir cherché longtemps avant de trouver qu'il fallait cliquer sur "Alignement" pour accéder aux options, on découvre qu'il faut chercher soi-même des serveurs proxies, et que donc ce logiciel n'offre rien de plus que les autres dans ce domaine ! Laissez donc tomber, et passons à autre chose.



Blubster (www.blubster.com) annonce, depuis sa version 2.5, un anonymat total. Par contre, impossible de trouver les spécifications détaillées de la technologie, ce qu'ils doivent sans doute justifier par la nécessité de protéger leurs secrets révolutionnaires... mais depuis quand quelqu'un désirant rester anonyme ferait confiance à une boîte noire magique ? Nous avons définitivement renoncé à l'instal-

er (et nous vous recommandons d'en faire autant) en découvrant que le programme tenait avec quelques petits spywares sympathiques comme le tristement célèbre Jator.

Sachant que Blubster ne permet, en plus, de ne télécharger que des fichiers musicaux, on peut passer, il n'y a pas grand-chose à voir. Si vraiment vous voulez l'essayer, téléchargez au moins une version sans spywares, à cette adresse par exemple : <http://drdamn.com/cleanclients/blubster250.shtml>.

Enfin, finalement, les réseaux P2P sont encore loin d'être à la hauteur du point de vue de l'anonymat, même si des efforts sont faits. Si vous deviez vraiment choisir aujourd'hui, je vous conseille encore Freenet, qui paraît être le projet le plus sérieux. Une autre source d'inquiétude vient de la légalité de tels réseaux. On pourrait en effet penser que puisque tout est encrypté et que Freenet n'a aucun contrôle possible sur le contenu du réseau, il ne peut pas être tenu responsable de ce qui y transite. Ce n'est malheureusement pas forcément vrai : le 1er juillet 2003, la RIAA a en effet emporté une victoire légale qui pourrait s'avérer importante contre le réseau P2P Joadster (anciennement Aimster). Ce dernier avait déjà perdu l'an dernier, mais avait fait appel en disant qu'il ne pouvait être tenu pour responsable de ce qui transitait sur son réseau : puisque tout était crypté, comment savoir que c'était illégal ? "Vous deviez vous en douter", a dit en gros le juge qui, il faut bien l'avouer, n'avait pas tout fait tort sur ce coup-là...

3 BLOQUER LES ADRESSES IP DU RIAA : UNE OPTION RISQUÉE

Une autre option consiste à se protéger spécifiquement des enquêtes de la RIAA et des autres associations anti-piratage en bloquant les adresses IP qu'elles utilisent. Le programme PeerGuardian (<http://methlabs.org/methlabs.htm>) est justement fait exactement pour ça. Un autre outil utile est le convertisseur, disponible sur <http://www.blue-ack.co.uk/convert.html>, qui permet de convertir les listes de blocage d'IP d'un format à un autre, pour les adapter à tous les principaux logiciels de P2P. La fonction de blocage d'IPs de la RIAA est même maintenant intégrée à la dernière version de Kazaa Lite (www.kazaaite.tk), le célèbre clone de Kazaa (sans les pubs et spywares).

Mais ne pensez pas que bloquer ces IPs vous rend invisible et vous donne le droit de faire ce que vous voulez sur le réseau : pendant que vous bloquez des IPs, les associations anti-piratage en acquièrent d'autres, ou mettent la main sur des proxys pour contourner le blocage. Et à ce jeu du chat et de la souris, c'est forcément la souris qui finit par se faire prendre. Alors certes, il y a beaucoup plus de souris que de chats et il y a peu de chances que ce soit vous, mais réfléchissez-y bien avant de prendre la décision !

PASSER PAR UN PROXY

Il y a bien une méthode plus sûre pour protéger votre identité, mais au détriment des performances : il s'agit bien sûr du proxy. La plupart des clients P2P permettent en effet de passer par un proxy – fonction présente à la base pour permettre la connexion depuis un réseau d'entreprise par exemple – mais que vous pouvez utiliser à votre avantage pour camoufler votre IP. Par exemple, sur le populaire eDonkey, cela se règle dans le menu "Options", puis "Proxy". Les proxys les plus populaires sont les proxys de type "Socks 4" ou "Socks 5" (voir l'article sur les proxys).

Par contre, utiliser un proxy présente deux inconvénients majeurs : la rapidité tout d'abord (ça risque de ramer sévèrement), et le fait d'être connecté indirectement au réseau, ce qui se manifeste sous eDonkey par exemple par un "low ID", ce qui implique des possibilités un peu plus limitées. Bref, l'anonymat en P2P est possible, mais il faut en payer le prix !

CHATTER SUR IRC

EST BIEN CONNU, LES RÉSEAUX DE BAVARDAGES IRC REGORSENT DE SYCHOPATHES, DE PÉDOPHILES ET DE PETITS JEUNES MAL INTENTIONNÉS. DANS CES CONDITIONS, ET MÊME SI CES IDÉES REÇUES SONT MANIFESTEMENT TRÈS EXAGÉRÉES, ÉVITER D'AFFICHER TROP VISIBLEMENT VOTRE VÉRITABLE IDENTITÉ EST PARFOIS UNE SAGE PRÉCAUTION.

VOS TRACES SUR IRC

Sur le réseau EFnet par exemple, on peut obtenir des infos sur quelqu'un par la commande :

```
whois nick
```

qui renvoie quelque chose du genre :

```
nick is lili@modem205.53-131-66.nowhere.videotron.ca * lili
nick on #hzv
nick using irc.homelien.no Who Cares
nick End of /WHOIS list.
```

Et on a facilement son adresse IP par :

```
dns nick
```

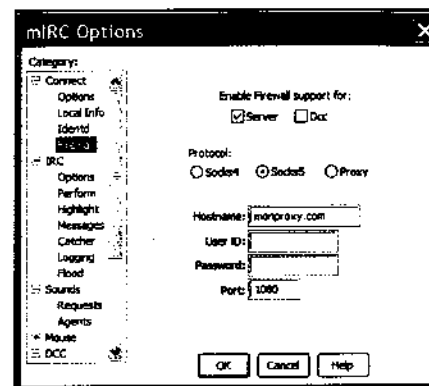
qui renvoie :

```
** Looking up modem205.53-131-66.nowhere.videotron.ca
** Resolved modem205.53-131-66.nowhere.videotron.ca to
6.140.24.37
```

Voilà exactement ce que l'on veut éviter que les autres apprennent sur nous.

COMMENT SE PROTÉGER

Le moyen le plus courant est d'utiliser un proxy (pour changer), ce qui se configure



sous mIRC dans les options, onglet "Firewall".

Il vous faut au moins cocher la case "Server" pour vous connecter au serveur via le proxy. Encore une fois, vous utiliserez le plus souvent les classiques proxies Socks 4 et 5, avec un risque cependant : de nombreux serveurs n'acceptent pas les proxies et vous renverront un message "banned" lors d'une tentative de connexion. Il n'y a pas grand-chose à faire dans ce cas, sinon essayer un autre serveur du même réseau... Pour détecter le fait que vous utilisez un proxy, les serveurs scannent votre adresse IP de connexion. Ne vous inquiétez donc pas si votre firewall s'affole, c'est parfaitement normal !

Une fois connecté, pensez à faire un /whois sur vous-même pour vérifier que le proxy a bien été configuré. Certains réseaux IRC offrent des fonctions d'anonymat pour protéger votre adresse. Vous pouvez généralement le découvrir dans le texte d'accueil du serveur ou en fouillant sur le site web du réseau, mais il n'y a pas de règle générale à ce sujet, et vous devrez chercher par vous-mêmes.

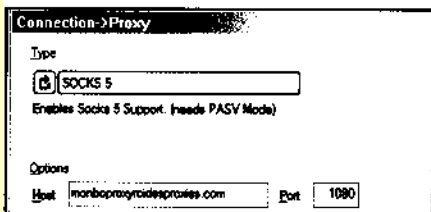
Enfin, une méthode classique utilisée sur IRC pour se camoufler est l'emploi d'un shell (un compte sur une machine – généralement Unix/Linux) pour se

LES TRANSFERTS DE FICHIERS PAR FTP

LES GROS TRANSFERTS DE FICHIER SE FONT RAREMENT PAR LE WEB. LE PROTOCOLE QUI EST LE PLUS UTILISÉ EST ALORS LE FTP. L'USAGE D'UN PROXY, LÀ ENCORE, NOUS SERA UTILE POUR CAMOUFLER NOTRE ADRESSE IP.

Le FTP est un autre domaine où l'anonymat n'est pas aisé, car on souhaite souvent obtenir un taux de transfert rapide, ce qui limite l'usage de proxies. C'est pourtant la meilleure solution pour l'anonymat.

Prenons l'exemple de celui qui est sans doute le meilleur client FTP entièrement gratuit, SmartFTP (www.smartftp.com) : les proxies s'activent dans le menu "Tools / Settings / Connection / Proxy".



Vous remarquerez qu'il y a différents types de proxies. Les plus classiques pour le FTP sont les proxies de type Socks (4 et 5, laissez tomber le 4a), ainsi que les proxies dits "FTP" du type "USER user@host:port". Cette syntaxe signifie que lorsqu'on utilise le proxy, on lui demande de nous connecter par exemple au serveur ftp.test.com sur le

port 2121 sous le nom d'utilisateur "anonymous" par la commande : USER anonymous@ftp.test.com:2121. Il existe différentes syntaxes, selon les proxies, c'est pour cela qu'il y a un grand nombre de choix dans SmartFTP. Vous aurez à expérimenter pour trouver le bon.

Évidemment, utiliser un proxy comporte l'inconvénient habituel de limiter sérieusement notre bande passante. De plus, en téléchargeant à travers le proxy, vous augmentez les risques de voir le proxy fermé à cause d'un débit trop important. Une solution intermédiaire consiste à vous connecter sur le serveur par le proxy, mais à télécharger directement, grâce au FXP ! Ainsi, l'adresse IP visible par l'administrateur du serveur FTP (celle logguée par le serveur) sera celle du proxy, tandis que les fichiers iront directement sur votre machine sans passer par le proxy.

Pour cela, vous devez faire du FXP (transfert de serveur à serveur), ce qui se fait en installant un serveur FTP sur votre machine, en vous connectant d'un côté sur le serveur FTP distant par le

proxy, de l'autre sur votre serveur local sans proxy, et en lançant un transfert FXP entre les deux. Pour plus de détails sur la technique du transfert FXP, se référer à des tutoriaux sur le FXP disponibles sur Internet, comme par exemple : <http://www.jtftp.net/ftpbasic.htm>

Cette technique n'est évidemment pas parfaite côté anonymat puisque votre adresse IP reste visible, une connexion TCP/IP directe s'établissant entre vous et le serveur FTP. Mais si personne ne surveille en temps réel, vous passerez sans doute inaperçu à moindre frais...

CYBER-CAFÉ, L'ARME ULTIME POUR L'ANONYMAT ?

Malgré tous les efforts que vous pourrez déployer, dans bien des cas, il sera toujours possible de remonter jusqu'à vous en retraçant l'origine des connexions, c'est-à-dire votre adresse IP (même si celle-ci est enfouie au fond d'obscurs logs de proxies), ou votre numéro de téléphone. Dans ces conditions, se connecter à partir d'un cyber-café est une solution attrayante pour ceux qui veulent être absolument intraquables (n'oubliez pas d'éviter quand même les caméras de surveillance, encore que ça risque de paraître louche dans un cybercafé, un client en lunettes de soleil devant son ordinateur). Évitez aussi toute activité pouvant mener vers vous : je me souviens qu'un hacker chevronné a ainsi été pris parce qu'il avait consulté son email (sur une messagerie type Hotmail) à partir du même cybercafé d'où il avait hacké quelques machines du Pentagone. Mais en prenant de bonnes précautions, c'est sans doute un bon moyen de minimiser les risques. Évidemment, le cyber-café n'est quand même pas la solution idéale : non seulement c'est cher, mais en plus rien ne vous dit que le client précédent ne vient pas d'installer un keylogger (enregistreur de touches du clavier) sur la machine que vous utilisez...

LE SYSTÈME D'EXPLOITATION, VOTRE PIRE ENNEMI ?

LE SYSTÈME D'EXPLOITATION DE MICROSOFT EST LE LOGICIEL QUI A SUSCITÉ LE PLUS DE SUSPICIONS ET DE RUMEURS, PLUS OU MOINS FONDÉES, SUR LE RESPECT DE LA VIE PRIVÉE. WINDOWS POSSÈDE EN EFFET UN CONTRÔLE COMPLET SUR VOTRE ORDINATEUR ET VOTRE CONNEXION INTERNET. DES PORTES DÉROBÉES PERMETTENT-ELLES À MICROSOFT D'ACCÉDER AUX INFORMATIONS VOUS CONCERNANT ?

Sil y a bien eu des tentatives en ce sens de la part de Microsoft, dans l'état actuel des choses, on peut dire que cela pourrait être bien pire. Les défenseurs des libertés individuelles veillent au grain, et Microsoft a souvent été contraint de se rétracter. Rassurez-vous donc, Microsoft n'est pas informé du nom des logiciels piratés présents sur votre disque dur ! Cependant, Windows reste sujet à de nombreuses failles de sécurité, et possède des fonctionnalités pouvant compromettre votre anonymat et permettre de vous tracer. Pas de panique, nous allons voir comment éliminer la majorité de ces menaces.

ENLEVER LE MOUCHARD DE MICROSOFT

Première chose à faire : si vous installez pour la première fois votre version de Windows, nous vous suggérons de ne pas mettre vos vrais noms et prénoms pour vous enregistrer, mais plutôt d'utiliser un pseudonyme. Dans le cas où vous auriez donné vos réels patronymes à votre ordinateur et donc à Microsoft, effectuez les manipulations suivantes pour changer ces coordonnées.

Dans le menu Démarrer>Exécuter, mettre "regedit" dans la fenêtre puis taper sur entrée. En cliquant, ouvrir la clé de registre "Hkey Local Machine>Software>Microsoft>Windows>Current version". Vous voilà sur les infos de l'utilisateur, que vous n'avez qu'à modifier.

Maintenant, désactivons le mouchard inclus dans votre système d'exploitation préféré, que ce soit Win 98, Millenium, 2000, ou XP. Il s'agit d'un contrôle qui permet aux

programmes d'avoir accès à un numéro d'identification unique, spécifique à votre ordinateur et à votre version de Windows, le GUID. Par exemple, un document Word créé à partir de votre machine portera ce numéro, qui permettra de vous tracer ! Il est impératif de s'en débarrasser.

Allez dans le menu Démarrer>Exécuter, puis tapez la commande suivante.

Pour Win98/Me :

```
regsvr32.exe -u c:\windows\system\regwizc.dll
```

Pour Win2K/XP :

```
regsvr32.exe -u c:\winnt\system32\regwizc.dll
```

Ou, pour XP, dans le cas où la précédente commande ne fonctionne pas :

```
regsvr32.exe -u regwizc.dll
```

Un petit message vous confirmera la réussite de l'opération.

Dans le cas où vous ne voudriez pas faire la manipulation par crainte de commettre une erreur, il existe un programme pour faire le travail à votre place. Microsoft a fourni un outil qui permet de désactiver ce mouchard... mais peut-on lui faire confiance à 100 % ? Vous pourrez le télécharger sur le site de Microsoft, sous la forme d'un Patch dénommé "Mise à jour de l'assistant d'inscription" (13Ko).

Puis, pour peaufiner le tout, vous pouvez chercher dans la base de registres les valeurs "chaîne" MSID et HWID et les supprimer. Faites auparavant une copie de sauvegarde de ces clefs que vous conserverez dans un endroit sûr.

NUMÉRO DE SÉRIE ANONYME

Dans le cas où vous n'aimeriez pas que le numéro de série de la version de votre système d'exploitation ne transparaisse, lancez le programme regedit et modifiez la clé :

```
Hkey_Local_Machine > Software > Microsoft > Windows > Current Version > Product Key
```

Remplacez-la par des XXXXXXXX. Pensez à sauvegarder l'original sur les papiers de votre PC, ça peut toujours être utile !

DÉSINSTALLATION DES DLL DÉLATRICES

Je vous invite aussi à supprimer certains fichiers DLL, qui sont des bibliothèques de fonctions partagées entre tous les programmes. Certaines sont en effet susceptibles d'ouvrir des trous de sécurité sur votre système ou de faciliter l'espionnage de vos

activités.

Pour cela il vous faut inscrire les noms donnés ci-dessous un par un dans la fenêtre "rechercher" puis "fichiers/dossiers" du menu "Démarrer". Dans "nommé", vous écrivez le nom de la DLL, et dans la fenêtre "rechercher dans" vous pouvez laisser votre disque dur "C".

Il existe une autre solution plus rapide. Pour retrouver toutes les DLL sur votre système, vous pouvez utiliser la commande "rechercher" dans votre menu de démarrage, puis entrer la ligne suivante :

*.dll

Ensuite, tapez sur la touche "entrée" et votre système mettra en route la recherche. Cela permettra à la commande de vous afficher toutes les DLL présentes sur votre disque dur. Pour simplifier le tout, faites un clic droit dessus puis cliquez sur "réorganiser les icônes" puis "par nom".

Je tiens à vous préciser que vous devez simplement supprimer ces DLL en les mettant dans la corbeille, et non pas les supprimer complètement dès maintenant, car il se peut qu'un programme vous en demande une particulièrement pour pouvoir fonctionner correctement. Auquel cas, vous la réintègrerez dans le système en un clic droit sur "restaurer" si le besoin s'en fait sentir. Vous supprimerez toutes les DLL inutiles dans quelques semaines.

Attention : nous vous mettons tout de même en garde contre le fait de supprimer des DLL de votre système sans les avoir sauvegardées au préalable ! Car même si votre Windows arrive à tourner sans elles, il est préférable de les avoir sous le coude en cas d'urgence... c'est ce que nous avons fait en les sauvegardant.

- adimage.dll
- advert.dll
- advpack.dll
- amcis.dll
- amcis2.dll
- amcompat.tlb
- amstream.dll
- anadsc.ocx
- anadscb.ocx
- browseui.dll
- htmldeng.exe
- ipcclient.dll
- msipcsv.exe
- html32.cnv qui est le convertisseur présent sur toutes les versions de Microsoft et qui ouvrirait une belle faille de sécurité. Si vous êtes webmaster, il est plus prudent de le patcher car vous risquez tôt ou tard d'en avoir besoin... sinon pour les autres, ceux qui

ne sont pas webmasters et/ou qui n'utilisent pas Internet Explorer ni Frontpage pour créer des pages web, mieux vaut le supprimer. Le patch (correctif) est disponible ici : <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-023.asp>

- mstask.exe (si vous ne vous servez pas des "tâches planifiées" pour mettre en service un programme à l'heure donnée, vous pouvez supprimer ce programme défaillant de votre système).
- mshtml.dll (la visionneuse HTML d'Internet Explorer, qui peut être présente plusieurs fois, surtout si vous avez installé une version de I.E. plus récente...).
- reginfo.txt
- regwizc.dll
- shdocvw.dll
- tfde.dll
- wupdinfo.dll (pour enlever la mise à jour automatique, qui est inutile sur win98 vu qu'il n'est plus mis à jour par Microsoft).

À noter que tous ces fichiers ne sont pas forcément présents sur un seul système, donc ne vous inquiétez pas si vous ne trouvez pas telle ou telle DLL. Précisons aussi que vous pourrez trouver deux DLL du même nom (comme mshtml.dll), surtout si vous avez mis à jour Internet Explorer par une version différente de celle que vous avez à l'origine.

Dans le dossier "System" de Windows, si vous avez désinstallé Internet Explorer, vous pouvez supprimer sans regret les DLL délatrices suivantes :

- BrowseIc.dll > Bibliothèque de l'interface utilisateur du navigateur Shell
- Browseui.dll > Bibliothèque de l'interface utilisateur du navigateur
- Browsewm.dll > BrowseWM Player
- Html32.cnv > Convertisseur html
- Mshta.exe > HTML Application host
- Mshtml.dll > la visionneuse html de Windows sujette à nombreuses failles
- Mshtml.ed.dll > Composant d'édition HTML Microsoft
- Mshtmler.dll > DLL de ressource du composant d'édition HTML
- SHDOCLC.dll > Bibliothèque d'objets et de contrôles de documents de l'environnement

Dans le dossier "Tasks" il y a ce fichier faillible, à supprimer si vous n'utilisez pas les tâches planifiées :

- MSTASK > Moteur du Planificateur de tâches

Pour le dossier VCM, vous avez ceci :

- MSHTML.dll > Visionneuse HTML Microsoft
- HTML32.cnv > Convertisseur Html faillible au plus haut point

- MSTASK > Moteur du Planificateur de tâches
- SHDOCVW.dll > Bibliothèque d'objets et de contrôles de documents de l'environnement
- WUPDMGR > Gestionnaire Windows Update de Windows 98

Bien sûr, si vous avez encore le navigateur, vous pouvez aussi supprimer certaines de ces DLL et autres fichiers faillibles. Toutefois, dans le cas où Internet Explorer se servirait de telle ou telle DLL, Windows refusera la suppression du fichier. Ceci pour vous confirmer que vous pouvez tenter de supprimer ces éléments malgré la présence de I.E. (toujours en ayant pensé à les avoir sauvegardés au préalable).

Si vous utilisez les services de Microsoft et associés tels que M.S.N., Hotmail, Windows Update, le Messenger de MSN, leurs serveurs risquent de vous réinstaller, plus ou moins à votre insu, les deux DLL principales "advpack" et "amstream". Même lorsque vous mettez à jour vos O.S. par l'installation de packs et de patches, Microsoft tente de vous "refiler" ces espions.

Pour les possesseurs de Windows 2000 et Millenium, vous trouverez des programmes pour protéger votre PC dans la rubrique téléchargement du site : <http://optimisersonpc.free.fr>.

LA MISE À JOUR DU SYSTÈME : AVEC OU SANS WINDOWS UPDATE ?

Microsoft propose sur ses systèmes d'exploitation une fonction de mise à jour automatique de celui-ci par le système "Windows Update". L'ordinateur se connecte tout seul au site de Microsoft pour récupérer les dernières mises à jour de sécurité. Windows 98 n'est cependant plus mis à jour par Windows Update, ce sujet ne le concerne donc plus.

Si l'intérêt de ce système est évident, il peut aussi poser divers problèmes. Tout d'abord, pour procéder à la mise à jour, le logiciel de Microsoft scanne votre disque dur afin de connaître les éléments qui sont installés sur votre système. La firme de Seattle dément toute récupération de vos infos personnelles, mais il s'agit là d'une question de confiance... D'autre part, il arrive que les mises à jour proposées soient moins fiables que le système à la base ! L'évolution informatique est parfois cahotique... Se ruer sur les correctifs mis à la disposition des internautes par Microsoft n'est pas toujours une bonne attitude. Il n'est pas rare qu'un meilleur patch soit mis à disposition quelques jours plus tard. Attendre un peu est donc une bonne démarche, tout en surveillant les news informatiques pour suivre les événements.

Dernier problème, peut-être le plus grave : dans certaines mises à jour, Microsoft peut inclure des DLL délatrices sans le révéler. Basiquement, cela signifie que Microsoft peut installer automatiquement n'importe quelle nouvelle fonctionnalité sur votre ordinateur... comme ce fut le cas dans le pack SP1 de Windows XP, qui a changé la vie (négativement) de nombreux utilisateurs ayant enregistré leur version de XP avec une clé trouvée sur Internet.

L'alternative à Windows Update est de ne pas utiliser cette fonction (et de désactiver la mise à jour automatique), mais plutôt de télécharger chaque mise à jour directement sur la page Microsoft concernée. Si vous aimez la lecture informatique, vous pouvez aussi acheter des magazines spécialisés qui proposent des Cd-roms avec des programmes et mises à jour inclus. Cette solution a l'inconvénient de vous obliger à vous tenir au courant tous les jours des nouveaux correctifs disponibles. De plus, vous devrez être à même d'en comprendre l'importance afin de savoir si vous êtes vulnérables, ou d'appliquer éventuellement une autre solution. Sinon, vous serez rapidement débordé par le nombre de correctifs.

Alors, mises à jour automatiques ou pas ? Bonne question, à laquelle nous ne pouvons pas répondre à votre place, mais dans tous les cas la prudence est de mise. Si vous désirez ne pas mettre à jour votre Windows par le biais de Windows Update, nous vous invitons à procéder comme suit. Lancez le programme regedit et éditez la clé :

HKey_Local_Machine>Software>Microsoft>Windows>CurrentVersion>Policies>Explorer

Créez-y une nouvelle valeur Dword dénommée "NoWindowsUpdate", double-cliquez dessus et donnez-lui la valeur 1.

Dès lors, plus de Windows Update possible. De plus, vous pouvez désactiver la mise à jour et la connexion automatiques d'Internet Explorer vers les serveurs de Microsoft, avec la manipulation suivante dans regedit :

HKey_Current_User>Software>Microsoft>Internet Explorer>Main
Ajoutez une clé Dword par un clic côté droit, en déroulant Edition>Nouveau>Valeur Dword. Nommez-la NoUpdateCheck. Puis double-cliquez dessus et donnez-lui la valeur 1.

Pour de nouveau permettre la recherche de mises à jour, il suffit de remettre la valeur à 0. Si Windows persiste à ne pas obtempérer, dans "Démarrer" puis "Exécuter", tapez : regsvr32wupinfo.dll

Cela provoquera la réinstallation de Windows Update.

NETTOYER WINDOWS XP

À noter que si les Windows 95, 98 et Me ainsi que 2000 sont "nettoyables" en étudiant le système, Microsoft a tout fait dans XP pour égarer les utilisateurs et/ou bidouilleurs en compactant cet O.S. Nombre de fonctions cachées sont présentes sur le système afin de vous tracer finement, voire même avoir la possibilité de bloquer plus ou moins partiellement certains programmes. Par exemple, dans le cadre d'utilisation de CD ou mp3 copiés, voire de cracks, l'équipe de Microsoft a imaginé bloquer un programme ou même le système complet, et a commencé à inclure cette possibilité.... Et nous ne parlons pas de la clé d'activation sur XP, qui est le contraire du respect de la vie privée des utilisateurs de cet "Operating System". Microsoft a réécrit différemment la nouvelle génération de clés d'activation de Windows XP, ainsi que le code de Windows XP qui permet de reconnaître cette clé. Ce nouveau code est intégré au Service Pack 1 (SP1) de Windows XP et permet à Microsoft de contrôler beaucoup mieux qui utilise ses logiciels, en interdisant aux versions considérées comme piratées de s'installer. La mise à jour prochaine de XP par la SP2, qui doit sortir des usines Microsoft en 2004, comportera sans aucun doute son lot d'espions et de failles intrusives...

Nous allons voir maintenant comment contourner quelques-uns de ces blocages. Mais tout d'abord, nous vous invitons à ne jamais fournir vos noms et prénoms, que ce soit dans les demandes de coordonnées lors du premier lancement du système ou sur les sites web qui peuvent vendre vos infos personnelles aux sociétés publicitaires.

Comment éviter de renvoyer ses infos personnelles lors d'une énième réactivation de Windows XP ?

Il suffit, avant d'effectuer la procédure du formatage et de la nouvelle installation, de sauvegarder le fichier wpa.dbl se trouvant dans C:\WINDOWS\SYSTEM32 sur un autre support. Après avoir réinstallé votre système, redémarrez en mode sans échec, renommez le fichier présent wpa.dbl en oldwpa.dbl, puis copiez le premier fichier wpa.dll que vous avez précédemment sauvegardé dans le dossier d'origine.

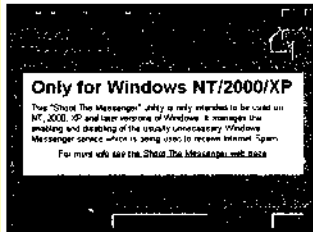
Nous allons maintenant désactiver certains services de Windows XP, qui présentent des risques pour un utilisateur qui tient à son intimité. Dans le menu Démarrer>Exécuter, entrez "service.msc", cliquez sur OK, et vous accéderez aux nombreux services de XP dont vous pourrez choisir d'interdire le fonctionnement permanent. À noter que si vous en avez besoin plus tard, vous pourrez le remettre en marche aussi facilement que lors de sa désactivation.

Nous vous conseillons de supprimer les services suivants :

- Accès à distance au Registre (autorise les manipulations à distance de votre base de

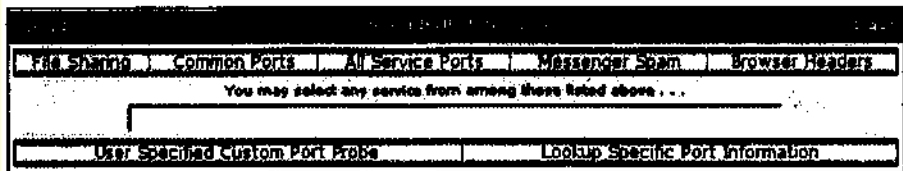
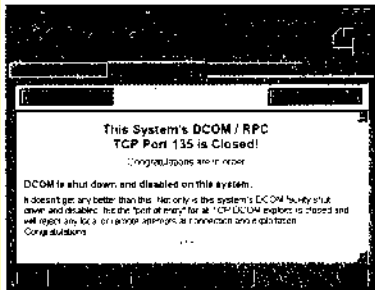
registres : à supprimer !)

- Affichage des messages (astuce anti-spam qui bloque les spammers qui utilisent ce service inutile, qui par ailleurs présente des trous de sécurité)
- Assistance TCP/IP NetBios (à désactiver si vous n'êtes pas sur un réseau NetBios)
- Explorateur d'ordinateur (si vous n'êtes pas sur un réseau local)
- Gestionnaire de session d'aide sur le bureau à distance (à désactiver si vous ne comptez pas utiliser l'aide à distance... sinon, il est de toute façon dangereux de le laisser en automatique)
- Horloge Windows (l'intérêt de la désactiver est d'éviter d'envoyer des infos aux serveurs de Microsoft)
- Mises à jour automatique (à désactiver si vous considérez que c'est à vous de choisir ce que vous désirez mettre à jour, et non pas à Microsoft. Mais n'oubliez pas alors de mettre à jour très régulièrement votre système !)
- Numéro de série du média portable (il s'agit d'un numéro permettant de vous tra-



cer sur internet, dont nous reparlerons dans une autre partie)

- Pare-feu de connexion Internet (vous pouvez l'utiliser, c'est mieux que rien. Mais nous vous conseillons plutôt d'utiliser Kério, plus efficace et gratuit)
- Partage de bureau à distance (et NetMeeting) à désactiver d'urgence !



- Partage de connexion Internet (à enlever si vous n'avez pas de réseau)
- Planificateur de tâches (si vous ne comptez pas l'utiliser pour planifier un lancement de programmes à une heure donnée, le mieux est de le désactiver)
- Service d'indexation
- Telnet (jamais utilisé)
- WebClient.

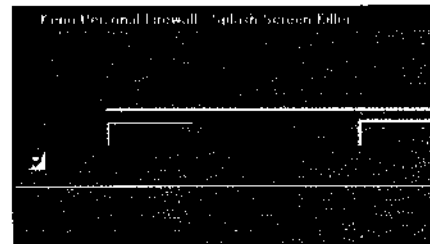
Il est prudent de désactiver aussi le service du rapport d'erreurs, qui s'envoie automatiquement aux serveurs de Microsoft. En effet, ce service donne à Microsoft bien plus d'informations sur votre ordinateur qu'il n'est nécessaire. Appuyez sur les touches "win" et "pause", où cliquez sur le poste de Travail avec le bouton droit, puis choisissez Propriétés. Dans l'Onglet Avancé, sélectionnez Rapport d'erreurs>Désactiver le rapport d'erreurs. Vous pouvez choisir d'être tout de même averti en cas d'erreur critique.

Enfin, pour désactiver le support de la compression zip intégré (il est plus prudent d'utiliser un logiciel externe spécialisé comme Winzip), cliquez sur Démarrer>Exécuter et entrez la commande suivante :

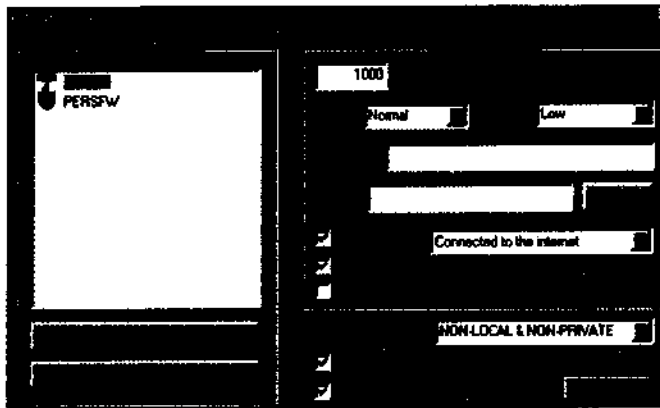
```
regsvr32 /u zipfldr.dll
```

Pour le réactiver :

```
regsvr32 zipfldr.dll
```



Pour désactiver nombre des espions inclus dans Windows XP, nous vous invitons à mettre en application les paragraphes précédents. Ensuite, nous vous recommandons l'utilisation de plusieurs logiciels gratuits qui vous permettront de vous protéger en les désactivant ou en les annihilant.



LES LOGICIELS GRATUITS QUI VONT SAUVER VOTRE PC

* Un excellent programme gratuit en langue française permet de supprimer facilement un bon nombre de spywares de Windows. Vous pourrez le télécharger sur le Net, il s'agit de XP-AntiSpy : <http://www.xp-antispay.org>

* Le site www.grc.com propose d'excellents freewares de protection comme **Shoot Messenger**, **XP Dite**, **Unplug'Pray**... qui combleront des failles de sécurité laissées ouvertes par Microsoft. Même la dernière faille sur le port 135 utilisée par le virus Blaster est testée par GRC. À tester d'urgence sur <http://grc.com/dcom/>. La liste générale des freewares de GRC est disponible sur <http://grc.com/freepopular.htm>. Vous trouverez même des tests online pour éprouver l'étanchéité de votre firewall... je vous laisse découvrir ce site :

* Vous avez aussi **LeakTest**, qui fonctionne comme un troyen installé sur votre PC afin de tester la fiabilité de votre firewall : <http://grc.com/lt/leaktest.htm>

* **SpyBot** en langue française, un équivalent de XP-Antipsy, que vous trouverez chez son traducteur français sur son site de protection informatique : <http://websec.arcady.fr>

Vous trouverez également les logiciels suivants sur le site <http://www.wilderssecurity.net> :

* **SpywareBlaster** joue la carte de la prévention en bloquant l'implantation de cookies délateurs et autres fichiers bavards.

* **MRU Blaster** et **ID Blaster** trompent les curieux qui vous tracent en modifiant vos numéros de série... Vos originaux, vous devez penser à les sauvegarder avant, cela va de soi.

* D'autres programmes de protection sont disponibles, dont un patch pour Windows Média Player qui bloque la lecture des scripts HTML dans le lecteur multimédia.

Cela dit, Windows Média Player se doit d'être désinstallé complètement via le Panneau de Configuration > Ajout/Suppression de programmes > Ajouter/Supprimer des composants Windows. En effet, c'est un grand bavard qui dit tout sur les fichiers audios et vidéos que vous détenez sur votre disque dur.

Pour bloquer les connexions indésirables, il vous faut un firewall sérieux comme Kério. Celui inclus dans XP n'est pas assez complet. Vous trouverez Kério sur : <http://www.kerio.com>

La version 2.15 est la plus stable de toutes, car les autres sont pour l'instant des bêtas. Si vous désirez franciser Kério, il existe un patch FR qui englobe aussi l'aide française sur : <http://www.toutfr.com>

Pour enlever le logo de démarrage de Kério, utilisez SplashKiller disponible en téléchargement sur :

<http://www.brightnova.com/downloads/KPFSplashKiller.exe>

<http://www.brightnova.com/kpf/>

Une astuce si vous désirez que Kério ne se lance que lors de votre connexion sur Internet, téléchargez NetRun ici :

<http://www.czarssoft.com/>

<http://www.ticon.net/~jclogon/NetRunSetup.exe>

* Pour votre protection antivirale, voici un produit gratuit et efficace :

<http://www.free-av.com>

Vous trouverez son patch de francisation sur le site d'Anticrah.net :

<http://www.anticrash.net>

ASTUCES EN BONUS

Pour une meilleure gestion de la mémoire, deux logiciels gratuits existent. Il s'agit de RamBoostXP en langue française :

<http://magic56.free.fr>

et de RamIdle en langue anglaise :

<http://www.tweaknow.com>

LES PROGRAMMES DE MICROSOFT... ET LES AUTRES

DES MOUCHARDS SONT DISSÉMINÉS DANS LES PROGRAMMES LES PLUS ANODINS. HEUREUSEMENT, IL EST SOUVENT POSSIBLE DE S'EN DÉBARRASSER.

LES LOGICIELS DE MICROSOFT

Dans les dernières versions de ses logiciels, Microsoft implante de plus en plus de mouchards et de moyens de tracer les utilisateurs. Non seulement dans ses systèmes d'exploitation, mais aussi dans son navigateur Internet Explorer, sa messagerie Outlook Express ainsi que ses logiciels de bureautique et autres outils multimédias tels que Windows Média Player.

• Office

Tout d'abord, pour Office XP, à l'aide de Regedit dans le menu "Edition/Nouveau/Valeur DWORD" :

- Rajouter des entrées nommées DWNeverUpload, DWNoExternalURL, DWNoFileCollection, DWNoSecondLevelCollection avec une valeur de 1 pour chaque utilisateur dans :

```
HKeyCurrentUser>Software>Policies>Microsoft>Office>10.0>Common  
- Rajouter ces mêmes entrées avec une valeur de 1 dans HKeyUser>Default>Software>Policies>Microsoft>Office>10.0>Common.
```

Pour nettoyer vos fichiers MS-Office 97 vous pouvez également vous procurer le gratuit Guideon (68 Ko), qui permet de supprimer a posteriori le numéro de série unique, présent dans tous les documents Word, Excel, etc. sans affecter les données du fichier. Vous pouvez le trouver sur :

<http://www.vecdev.com/guideon.html>

Si vous désirez télécharger les patches anti-mouchards et sécurité fournis par Microsoft (!) pour les suites d'Office, voici l'adresse :

<http://office.microsoft.com/france/ProductUpdates/default.aspx>

À noter que le site français essaie de scanner votre disque dur afin de chercher une version d'Office. ce n'est pas le cas du site suivant, en anglais : <http://office.microsoft.com/Downloads/default.aspx>

Ou bien, si vous ne voulez pas chercher le lien, vous pourrez télécharger le patch "Unique Identifier Removal Tool" (140 Ko) qui supprime le GUI, autrement appelé "mouchard" d'Office 97 (identifiant unique présent dans tous les documents que vous créez, et qui permet donc de vous tracer). Téléchargez-le directement sur le site en langue anglaise de Microsoft :

http://office.microsoft.com/downloads/9798/pf_setup.aspx

• Internet Explorer

Il faut désactiver le rapport d'erreur, qui renvoie beaucoup trop d'informations sur votre système à Microsoft... en particulier le contenu de la mémoire du navigateur au moment où l'erreur a eu lieu !

Pour Internet Explorer 5.x, dans le "Panneau de configuration" choisir "Ajouter/Supprimer des programmes". Sélectionner "Internet Explorer Error Reporting" et cliquer "Ajouter/Supprimer" ou "Modifier/Supprimer" selon les versions de Windows.

Pour Internet Explorer 6.0 sur Windows XP, dans le "Panneau de configuration", choisir "Performances et maintenance". Sélectionner "Système", onglet "Avan-

cé", bouton "Rapport d'erreurs" et : soit sélectionner "Désactiver le rapport d'erreurs", soit décocher "Système d'exploitation Windows" et/ou "Programmes" selon la politique de sécurité.

Pour Internet Explorer 6.0 pour Windows 98/2000, ouvrez Regedit dans le menu "Edition/Nouveau/Valeur DWORD". Rajoutez l'entrée suivante, avec une valeur de 0, dans HKeyLocalMachine>Software>Microsoft>Internet Explorer>Main : IEWatsonEnabled.

Pour se débarrasser des URLs dans Internet Explorer, il est également nécessaire de modifier la base de registres. Cliquez sur le bouton Démarrer, puis Exécuter : regedit.exe. Allez sur HKEY_CURRENT_USER/Explorer. Dans le panneau de droite apparaissent toutes les adresses, sous la forme url1=, url2=, etc... Vous pouvez supprimer les adresses que vous ne voulez pas voir apparaître.

• MSAGENT

Si vous avez le dossier MSAGENT dans C:\Windows, vous pouvez le supprimer après l'avoir sauvegardé dans un dossier extérieur. Regardons de plus près la DLL MSLWTTTS.dll, incluse parmi les autres de ce dossier. On découvre que son nom long est : Microsoft Agent International DLL Registry Update and Installation Control...

Au passage, signalons que dans le dossier Windows, vous pouvez aussi supprimer "wscript" et "cscript" qui affichent

les scripts .wsh et .vbs, dont l'unique utilité semble être de porter des virus !

• Windows Média Player

Ce logiciel musical installé par défaut sur Windows est aussi une véritable passoire en scripts HTML et on y a découvert de nombreuses failles de sécurité. Mais rentrons quelques instants dans notre mode "paranoïaque". Ses multiples versions sont réputées pour comporter des fonctions de "caftage" qui permettraient de savoir si la musique que vous écoutez a été acquise de façon légale ou pas... La dernière version en date au moment de l'écriture de ce guide, la numéro 9, serait truffée de fichiers délateurs destinés à connaître la musique que vous écoutez ainsi que les films que vous regardez, mais surtout les conditions d'obtention de vos fichiers médiatiques. Sur Windows XP, il y aurait même la possibilité de bloquer le système à distance ou de condamner à jamais l'utilisation des fichiers audio.

Même en quittant le mode paranoïaque, il est vrai que c'est vers quoi tend de plus en plus Microsoft, qui ne s'en cache pas dans ses déclarations officielles. Et une chose au moins est prouvée : le Media Player permet de vous tracer sur Internet en vous attribuant un numéro d'identifiant unique (un peu comme le GUID de Windows et de la suite Office), qui est accessible aux sites web que vous visitez !

Il faut donc supprimer tout de suite cet espion. Dans ce logiciel, allez dans le menu Outils/Options, et décochez les

cases "Autoriser les sites Internet à identifier le Lecteur de manière unique" et "Acquisition automatique des licences". La meilleure solution reste de désinstaller au plus vite ce logiciel. Si par hasard vous désirez le conserver sur votre PC, ne vous en servez pas et bloquez-le avec votre firewall comme vous l'avez fait (nous l'espérons) pour Internet Explorer.

Vous avez à votre disposition Winamp pour la musique, qui est le lecteur audio de référence, ainsi que BS Player pour la vidéo. Ces deux programmes sont excellents. Toutefois en ajoutant un plug-in, Winamp peut même lire vos vidéos sous de nombreux formats. Un seul programme pour de nombreuses fonctions audio et vidéo, autant en profiter !
<http://www.winamp.com>
<http://www.bsplayer.com>

Nous avons déjà parlé d'Outlook Express, logiciel de messagerie parmi les plus vulnérables aux virus et autres scripts HTML d'Internet Explorer qui est peu sécurisé et comporte de nombreuses failles, mais d'autres logiciels de la firme de Seattle sont aussi mis en cause sur l'autel de l'insécurité. Word par exemple permet, pour qui sait s'en servir, de connaître le nom de l'utilisateur de ce programme si ce dernier a commis l'erreur de s'enregistrer sous son véritable nom. Il est simple pour Microsoft de savoir quelle version vous utilisez, d'avoir vos coordonnées et de connaître l'utilisation légale ou pas de leur programme. Et dire que certains créent des sites web avec Word !

Évitez donc les programmes de Microsoft et trouvez-leur des équivalents, vous ne pourrez qu'être satisfait de cette démarche, que ce soit au niveau de la sécurité de votre PC que pour votre anonymat. Allez faire un tour chez les logiciels gratuits et vous trouverez des programmes fiables comme AbiSource ou OpenOffice dans les traitements de texte. Ils remplacent correctement la suite Office de Microsoft. Ces suites gratuites et complètes existent en français ou en langue anglaise, et certaines sont même open-source. À trouver sur :
<http://www.openoffice.org>
<http://www.abisource.com>

LES AUTRES LOGICIELS

De nombreux concepteurs de programmes s'appuient sur des fonctions avancées des DLL de Microsoft pour effectuer leurs tâches, ce qui pose des problèmes au niveau de la sécurité. D'autres intègrent leurs propres mouchards... Pour qu'un logiciel soit sécurisé et anonyme, il se doit – mais ce n'est pas suffisant – d'utiliser le moins possible les fonctionnalités offertes par Microsoft. La voie sécuritaire est difficile, mais plus vous serez exigeant plus vous serez à l'abri.

En premier lieu, bannissez les programmes de sécurité déclinés en deux versions : la "light" qui est gratuite mais qui comporte moins d'options, et la version payante dite "pro". L'éditeur compte sur la version gratuite pour vous "appâter", en vue de vous proposer la version plus évoluée. Automatiquement, la ver-

sion gratuite n'est pas aussi efficace que la payante. Cela va de soi. La dernière faille de sécurité du firewall Zone Alarm a mis ce problème aux premières loges alors que nous le dénonçons depuis longtemps. De nombreux utilisateurs de cette version ont été bernés et se croyaient protégés alors qu'une faille critique a été découverte, et que l'éditeur ZoneLabs ne faisait rien pour la boucher car cela concernait la version gratuite ! Vous ne payez pas ? Donc vous n'avez pas droit à la garantie de votre sécurité et ni de votre anonymat chez ZoneLabs... mais je peux vous confirmer qu'ils ne sont pas les seuls à penser de cette façon. Dès à présent, utilisez le principe de précaution et ne tombez plus dans le piège : achetez la version Pro ou mieux, rabattez-vous sur un autre logiciel purement gratuit.

Donnons maintenant quelques exemples de programmes connus pour poser problème.

* **RealPlayer**, dans le passé, a eu les mêmes tendances à "l'espionnage" que Microsoft... Méfiance donc lors de l'utilisation de ce logiciel.

* **Kazaa**, le top des logiciels les plus téléchargés, comporte des espions. Déjà, pour ce premier point, il est à bannir ! Mais le plus beau de l'histoire, c'est que les versions de ce programme dépouillées des espions envahissants, comme Kazaa Lite, continuent d'être fragiles, puisqu'elles utilisent toutes au maximum les DLL de Windows et d'I.E. De ce fait, votre sécurité est mise en

danger : nombre de petits malins connaissent les vulnérabilités qui en découlent.

EDonkey ou son pendant open-source E-Mule sont aussi suspects, car ils ont besoin d'I.E. pour fonctionner !

* **mlrc**, le fameux logiciel permettant l'accès au réseau I.R.C. (Internet Relay Chat), ne comporte pas d'espion, mais il est très souvent pris pour cible par les pirates. Plusieurs trous de sécurité ont été découverts. Je vous invite à télécharger d'autres programmes, en langue anglaise, tels Virc ou HydraIRC, qui sauront mieux vous protéger que mlrc.

Mais pensez à configurer finement le programme que vous utilisez, car beaucoup de "lamers" se dissimulent sur des canaux où ils ont envie de montrer à leur entourage que ce sont des pros du clavier. Donc, vérifiez avant toute utilisation les options de votre programme, et bannissez-y tout remplissage de vos véritables coordonnées. De plus :

- refusez toute réception automatique de fichier. Même si vous récupérez le fichier d'un ami, réalisez un petit scan antivirus sur lui avant de l'ouvrir.
- mettez un pseudo ou une fausse identité dans les cases vous le demandant.
- pour les dames, si vous désirez être tranquilles, prenez un pseudonyme masculin.
- et bien entendu, assurez-vous d'avoir installé sur votre PC un antivirus mis à jour fréquemment et un firewall pour vous protéger.

* Les antivirus

Certains programmes, comme ceux de Symantec, s'implantent dans les dossiers de Windows comme pour mieux s'infiltrer. En particulier, ils intègrent des composants ActiveX. Nous le savons tous, ce type de fichiers peut procéder à toute opération sans votre accord sur votre disque dur et est accessible via Internet. Les failles de sécurité qui y sont souvent présentes peuvent permettre à un pirate de détourner votre ordinateur, et – comble du paradoxe – d'y installer un virus !

Vous vous croyez à l'abri parce que vous avez un produit antivirus lourd et complexe sur votre PC... Ce n'est pas forcément le cas. Préférez les logiciels simples, sans fioritures, mais efficaces ! Et en tout cas, surtout pas ceux qui utilisent des composants ActiveX.

La liste n'est évidemment pas finie... Votre meilleure arme, c'est vous-même. Avant d'utiliser un nouveau logiciel, renseignez-vous sur les pratiques de son éditeur, et fouillez dans les options du programme. Ensuite, tenez-vous au courant des problèmes qui y seraient découverts en vous inscrivant à des forums et à des listes de discussion sur Internet, dédiés à l'anonymat et à la sécurité, comme les listes du site www.securityfocus.com (qui appartient à... Symantec !).

INDISPENSABLE LE CD-ROM OFFICIEL DE THE HACKADEMY SCHOOL



LE CD THE HACKADEMY SCHOOL

INCLUS TOUS LES LOGICIELS
POUR ÊTRE ANONYME SUR INTERNET
voir page suivante

