Les dossiers pratiques de www.anonymat.org

Comment être Anonyme sur le Web ?

2e Edition du 01 septembre 2000

Table des matières

I.- Introduction

Pourquoi vouloir absolument chercher à rester anonyme ? non pas (et surtout pas) pour assouvir quelques perversions malsaines ou se rendre coupable d'actes moralement condamnables, mais simplement pour permettre au Netoyen (citoyen du Net) responsable que nous sommes, de pouvoir jouir de son droit légitime et légal (au vue de la loi Européenne) à l'anonymat parce que c'est par là que passe le respect de la vie privée et des libertés individuelles.

L'anonymat est un droit inaliénable et non un gadget ou un privilège futile. Revendiquons nos droits pour que l'Internet reste et demeure une zone de liberté.

Ce dossier, remis à jour régulièrement, est une compilation de connaissances sur les techniques d'anonymat. Vous pouvez l'enrichir de vos expériences et connaissances et y apporter d'éventuelles corrections ou précisions.

Les bases juridiques de l'anonymat

Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales.

Article 8

1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

Article 10

1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

II.- Les techniques d'identifications.

Lorsque vous surfez sur le Web, rien ne garantit que votre anonymat soit préservé bien au contraire !

Quels sont les acteurs de ces traques et quels en sont les enjeux ? nombreux sont les acteurs indélicats qui ont intérêt à vous identifier :

- Les régies publicitaires en ligne (dont la tristement célèbre et très répandu *DoubleClick*, *Naviant*, etc.) tentent de répertorier vos goûts et vos habitudes d'achats dans une immense base de donnée nominative mondiale, à des fins Marketing.

- Les éditeurs d'espiogiciels (ou SpyWare) qui envoient des informations personnelles à votre insu, via des mouchards présents dans de nombreux petits utilitaires (ou parfois même dans de « grandes » applications) dont certains très connus, à des fins statistiques ou Marketing.

- Les services de renseignement des grands pays industrialisés qui « écoutent » les télécommunications du monde entier à des fins de sécurité ou d'espionnage industriel.

Il existe de nombreuses techniques d'identification des internautes, dont nous apprendrons à nous protéger :

- Les *cookies*, certainement la méthode plus répandue. Ces petits fichiers de texte contiennent un numéro d'identification, non-nominatif, et des statistiques propre à vos visites sur le site concerné (pages consultées, nombre de visites, actions effectuées, etc.). Ils peuvent rester des mois sur votre disque dur. Certains sont utiles (Caddies virtuels qui mémorisent vos achats sur un site marchand), d'autres servent à vous pister ! Nous verront des outils de filtrage qui savent faire la différence…

- L'adresse IP de l'internaute. Au début de chaque connexion, chaque utilisateur se voit attribuer dynamiquement un numéro sur 32 bits (série de 4 chiffres de 1 à 255) qui identifie votre ordinateur sur l'Internet. Ce numéro permet de récupérer le contenu d'une page Web, suite à la requête de l'utilisateur : c'est grâce à lui que le serveur Web expédie la bonne page Web à la bonne personne. Vous pister grace à votre adresse IP est un jeu d'enfant, toutefois cette technique est moins fiable : dans certains cas, l'adresse IP de l'internaute est amenée à changer régulièrement (cas d'une connexion RTC par Modem) ou à être substituée (cas de machines se trouvant derrière un firewall et présentant la même adresse IP).

- Les « Web bugs », ces *cookies* intelligents sont présents sous forme d'une image invisible et indétectable constituée d'un unique pixel présent, soit dans un E-mail au format HTML (appelé « Taupe », généralement une publicité non sollicitée), qui vous est envoyé anodinement, soit sur certains sites Web (notamment ceux présentant des publicités DoubleClick) voire dans des groupes de discussions. Si vous utilisez un client de messagerie capable de visualiser les messages en HTML (comme OutLook) cette « image » provoque la connexion automatique à un serveur distant qui est capable de converser avec tous les cookies de la même société présents sur votre disque (et d'en créer de nouveaux !) et peut récupérer

en même temps votre adresse E-mail et votre adresse IP !
Cette technique est décrite en détail (et en Anglais) sur le site Web de Richard Smith expert en sécurité informatique et découvreur de nombreux mouchards dont celui de Windows® 98.

- L'espionnage, à la volée, de données informatiques tels que les E-mails. Nous essayerons de vous donner quelques conseils pour tromper la vigilance du réseau Echelon par exemple dont la technique de base repose sur la détection de mots-clefs « sensibles » dans vos messages.
Pour plus d'informations voir notre dossier sur le réseau Echelon.

De même, chaque site que vous visitez peut connaître l'adresse IP de votre ordinateur, le site d'où vous venez, le type de connexion, votre système d'exploitation et le navigateur utilisé et bien d'autres choses encore. Tout cela grâce aux variables d'environnement émises par votre navigateur préféré. Pour s'en faire une idée, vous pouvez aller voir le site Web de la Cnil ou le site américain BrowsInfo encore plus complet. Ces informations servent à adapter les pages Web aux différentes plateformes du client mais peuvent être utilisées à d'autres fins notamment d'identification.

Chaque information personnelle présente sur votre machine est autant d'identifiant qui représente un danger pour votre vie privée :

- La base de registration de Windows® fourmille de nombreuses informations pouvant vous identifier (nom, adresse e-mail, numéro de série de Windows®) et pouvant être lu par un VbScript ou un ActiveX inclut dans une page Web.

- L'adresse MAC unique de votre carte réseau peut vous trahir ! d'autant qu'elle est insérée automatiquement dans les documents MS-Office® 97 (un patch existe).

- Le Processor Serial Number, ce numéro de série intégré au Pentium® III, peut vous identifier, si vous ne l'avez désactivé dans le BIOS de votre ordinateur ou à l'aide d'un utilitaire que vous trouverez dans notre rubrique « Patchs ».

Le but de cette *traque sur Internet* ? La plupart du temps le Marketing. Les fichiers ainsi créés peuvent-être loués ou vendus aux entreprises à des fins de marketing direct. La valeur d'un e-mail ? Entre 0,60 et 1,50 F. Plus l'info est ciblée et plus le fichier vaut cher, d'où cette course effrénée à l'information chez les Cyberannonceurs.

Même votre fournisseur d'accès vous espionne : « Quand un abonné de notre service tape une adresse (ndlr : d'un site Web) dans son navigateur un logiciel compare cette adresse avec celle d'un annuaire de type Yahoo, de cette manière, nous savons à quel thème appartient cette adresse cela nous permet d'établir des profils » - *Hervé Simonin* Directeur général de **Freesbee**, fournisseur d'accès gratuit.

III.- Les Parades.

A.- La navigation sur le Web

1.- Configurer au mieux son navigateur.

La configuration par défaut de votre navigateur Internet n'assure pas un niveau de sécurité optimal.

Configuration par défaut :

- Les *cookies* sont acceptés
- Le Scripting est activé (JavaScript et VBScript)
- Les *applets* Java et les ActiveX sont exécutés.

N'hésitez pas à jouer sur les options de la boîte de dialogue des *Paramètres de sécurité* afin de désactiver ou demander confirmation pour le Scripting, les *applets* Java ou les ActiveX.

Outlook Express vous permet également d'insérer l'adresse de sites sensibles (par exemple ayant des publicités *DoubleClick* ou celle de sites « Underground ») dans une section plus restrictive au niveau de sécurité très élevé, n'hésitez pas à utiliser cette possibilité en allant dans le menu *Outils*, sous-menu *Options Internet* Onglet *Sécurité*, cliquer sur l'icône *sites sensibles* puis sur le bouton *Sites* et saisir l'URL du site.

Puis indiquons à *Outlook Express* de ne pas lancer de code JavaScript attaché à un E-mail :

Dans *Outlook Express*, cliquez sur *Outils*, *Options*, *Sécurité* et *Zone sites sensibles* puis sur OK. Dans le Panneau de configuration cliquez sur l'icône *Options Internet*, puis sur *Sécurité*, *Sites sensibles*, *Personnaliser le niveau*. Dans la boîte de dialogue qui s'affiche, désactivez l'option "*Active Scripting*" puis validez les modifications.

2.- Gérer ses cookies.

Le *cookies* ont été créés pour éviter de stocker des masses d'informations énormes sur les serveurs des sites Web, ces informations sont donc déportées sur les machines clientes pour plus de souplesse dans leur gestion.

Les *cookies* sont placés en mémoire vive et ne sont inscrits sur le disque dur que lorsque l'on quitte son navigateur Internet.

Sous la pression des associations américaines et européennes de défense de la vie privée, les fabricants de logiciels ont été **contraints** d'intégrer des fonctions de désactivation des *cookies* au sein de leurs navigateurs.

Cependant, je vous déconseille fortement de désactiver les *cookies* car de nombreux sites vous resteront inaccessibles. Nous utiliserons plutôt un *gestionnaire de cookies* que vous trouverez dans la section « outils » du site. Ceux-ci analysent les *cookies* entrant, en tâche de fond et en temps réel, et les acceptent ou les rejettent en fonction de leurs utilisation.

En l'absence de *Gestionnaire de cookies*, supprimez **systématiquement** vos cookies à chaque fin de cession. Pour ce faire :

Sous ***Netscape*** recherchez le fichier 'cookies.txt' (C:\Program Files\Netscape\...\cookies.txt) et éditez le en double-cliquant dessus. Effacez toutes les entrées sous la ligne 'file! Do not edit.'.

Sous ***Internet Explorer*** supprimez manuellement tous les fichiers (sauf index.dat) présents dans le dossier "C:\Windows\Cookies" ou rajoutez cette ligne à la fin de votre fichier "autoexec.bat" :

```
ECHO O | DEL C:\WINDOWS\COOKIES\*.*
```

A chaque démarrage, tous les fichiers présents dans le dossier « Cookies » du répertoire « Windows » seront automatiquement effacés !

Les « Web bugs »

Comment se prémunir de ces *cookies* intelligents constitués d'une image gif de 1 pixel que nous avons décrit dans le chapitre II. car ils sont indétectables par les filtres *anti-cookies* ?

Les navigateurs de dernière génération permettent une gestion plus fine des *cookies* :

Microsoft nous en donne la possibilité avec *Internet Explorer* 5.5, au grand Dam des cyberannonceurs. Ce dernier expérimente une fonction qui permet à l'internaute de rejeter les *cookies* ne provenant pas du site Web qu'il est en train de visiter.

Dans *Netscape* 6, une option intitulée « *Accepter uniquement les cookies renvoyés au serveur d'origine* », autorise la lecture d'un *cookie* que par le serveur qui l'a émis. Evitant la lecture de *cookies* de la même société mais qui auraient été émis par différents serveurs de différents sites (cas DoubleClick).

3.- Les Proxies.

Certains sites Web servent de serveurs relais : Ils vous proposent de se connecter sur un serveur (Web ou parfois FTP) à votre place puis vous retransmettent les données. Pour le serveur distant le serveur *proxy* est le client, vous êtes inexistant donc anonyme.

Faisant les requêtes en leur nom, ils interceptent *cookies*, *applets* Java et JavaScripts/VBScripts ainsi que les ActiveX et les bandeaux publicitaires, vous évitant ainsi d'être identifié et donc « Spammé », puis ils vous renvoient les pages « anonymisées » en léger différé à peine perceptible.

Toutefois, il arrive que certains services augmentent la temporisation de la redirection des pages vers votre navigateur, en contrepartie de la gratuité, pour vous inciter à vous abonner.

Le service Web identifie l'adresse IP et les différentes informations (comme l'adresse e-mail ou l'historique des navigations) du serveur proxy et non les votres !

La confidentialité est également assurée du côté de votre FAI qui ignore tout de votre parcours sur le Web, chaque requête ayant lieu sur le *proxy*, qui se charge de vous connecter sur le site désiré.
Sachez toutefois sachez qu'en cas d'enquête judicaire (très) sérieuse votre véritable adresse IP sera retrouvée.

Vérifiez que le *proxy* que vous utilisez soit bien anonyme, afin qu'il ne transmette pas votre adresse IP au serveur sur lequel vous voulez vous connecter !

A cette fin je vous conseille de vous connecter, via le *proxy* de votre choix, sur l'un des sites de test que vous trouverez dans notre « annuaire des sites d'anonymat », qui vous renverra votre adresse IP, qui doit être différente de celle que votre FAI vous a attribué en début de connexion et que vous pouvez obtenir grace à l'utilitaire de « Configuration IP » (winipcfg.exe) de Windows© 95/98 ou en tapant *ipconfig* sous la fenêtre de commande de Windows© 2000.

Bien sur, le serveur *proxy* enregistrera votre passage dans ses *logs* mais pour tous les services visités vous serez anonymes excepter les accès FTP, les messageries en direct (ICQ, AOL messenger), ou encore les sites « Webmail » comme MS-Hotmail.

Enfin, sachez que certains services tiennent à jour une liste « noire » d'adresses IP de *proxies*. Dans ce cas le site refusera la connexion. Il vous suffira d'utiliser les services d'un autre *proxy*.

Il existe différentes façons d'exploiter les serveurs *proxy* :

- Les sites Web d'anonymat, comme *Anonymizer.com* ou *SpaceProxy* utilisent des serveurs *proxy* pour masquer votre navigation. Dans ce cas on saisie directement l'adresse du site où l'on souhaite naviguer incognito dans un champs prévu à cet effet sur le site Web du service. Dans la rubrique « Annuaire des sites d'anonymat » vous trouverez un grand choix de tels sites souvent gratuits.

- Une ligne de commande à placer dans votre navigateur dans la section « *Paramètres du réseau local* » d'*Internet Explorer* par exemple. La plupart des sites Web proposent cette possibilité d'intégrer, dans votre navigateur, une ligne de commande vers le *proxy*. Avantage : pas besoin d'aller sur le site Web du

service, tapez votre adresse normalement dans votre navigateur et le tour est joué ! ex : http://proxy.spaceproxy.com:8080 ou www.anonymizer.com:8080 (8080 est le numéro du port généralement utilisé par les *proxies*).

- Les applications qui fonctionnent en tâche de fond comme *Anonymity 4Proxy* (A4P) qui offre une liste de serveurs *proxy* avec une gestion centralisée évitant ainsi d'avoir besoin de (re)paramètrer son navigateur et qui permet également de substituer votre adressse IP contre une adresse IP anonyme.

- Certaines formules mixtes conjuguent logiciel tournant en tâche de fond + *proxy* Web comme *Freedom* ou *PrivadaProxy*. (voir la rubrique « annuaire des sites d'anonymat »). Leur niveau de sécurité est généralement des plus élevé mais ces solutions sont généralement payantes.

Vous trouverez une liste à jour de proxies sur : http://proxy.nikto.net/all_list.htm

Dans tous ces cas de figure le principe de fonctionnement des *proxies* est identique à ce que nous avons décrit.

Surfez sans laisser de traces

De plus en plus de fournisseurs d'accès Internet (FAI), utilisent des *Proxies*, sorte de gros disque dur qui font offices de mémoire cache pour stocker les pages des sites les plus sollicités, en vue d'accélérer les requêtes à ces sites par les utilisateurs.

Si pour une raison ou pour une autre, vous ne désiriez pas que les pages ou les images d'un site soient stockées (même provisoirement) sur le *proxy* de votre FAI, vous avez la possibilité de configurer une connexion directe à Internet :

Sous Netscape : *Préférences*, *Avancées*, *Proxy*, *connexion directe à internet,* sans passer par le proxy donc sans laisser de traces.

Sachez cependant que vous perdrez l'avantage de la célérité de la connexion aux sites Web les plus populaires qui sont généralement présents dans leur globalité dans les *proxies* des FAI mais que vous gagnerez du temps pour les autres sites car à chaque requête une recherche est effectuée dans le *proxy* afin de déterminer si la page désirée y est présente ou non.

Les Proxies anonymes publics

Ces *proxies* anonymes et gratuits, sans login ni mot de passe, s'utilisent le plus souvent en ligne de commande à intégrer dans votre navigateur.

Souvent issues d'entreprises ou d'administrations, ils sont théoriquement censés être fermés au public ce qui explique que quelques *proxies* ne fonctionnent qu'à certains moments de la journée, ou à certaines périodes.

Vous trouverez une liste de *proxies anonymes* régulièrement mis à jour sur :

http://proxy.nikto.net/anon_list.htm

et également sur les sites *undergrounds* suivants :

http://www.novelsoft.com/dark/proxy/
http://tools.rosinstrument.com/proxy/proxiesn.htm

Toutefois vous pouvez vous inscrire à la liste « *proxies* » de e-groups afin de recevoir une liste de *proxies* testés, accompagnée de liens vous permettant de les vérifier.
Pour vous abonner envoyez simplement un e-mail à :

mailto:proxies-subscribe@egroups.com

Si vous avez envie de surfer anonymement sur le net, voici un exemple pratique qui met en œuvre ces proxies anonymes :

1.- Allez dans *Internet Explorer* 4 ou 5. Allez dans "*Outils*", sous-menu "*Options Internet*", onglet "*Connexion*". Cliquez sur le bouton "*Paramètres LAN*" ("Utiliser un serveur proxy" sous IE4)
Placez-vous dans les paramètres "*avancés*" et entrez l'URL d'un serveur proxy anonyme (voir ci-dessous) dans le champ « HTTP » en y ajoutant le numéro du port associé (généralement 8080).

Cliquez sur la case "*Utiliser le même serveur proxy pour tous les protocoles*" (les serveurs anonyme ci-dessous fonctionnent avec les protocoles HTTP, FTP et Gopher)

Dans *Netscape* : allez dans les menus *Editer*, *Preferences*, *Avançées*, *Proxies*, puis « *Configuration manuelle du proxy* » et cliquez sur *Voir*, remplissez la zone « HTTP » et « Port ».

2.- Inscrivez-vous à un fournisseur d'accès gratuit (FAI) du genre "fnac.net" (en réalité Mageos.com dont le CD-Rom est disponible gratuitement). Pourquoi Fnac.net ? parce que l'inscription s'effectue en ligne et votre identité n'est pas vérifiée (pas de numéro de Carte de paiement à saisir, pas de confirmation par courrier). Pensez à donner un nom de compte bidon (surtout pas votre nom !) et pensez à faire précéder votre numéro d'accès par le "36 51" afin de camoufler l'affichage éventuel votre numéro de téléphone (des fois que votre FAI lorgne dessus !). De cette façon, seuls les Pompiers, la Police et l'Elysée peuvent voir votre numéro directement...
Pour les paranos, vous pouvez créer votre compte à partir d'un Cyber-café.

Il ne vous reste plus qu'à insérer le numéro de téléphone du FAI gratuit précédé du "36 51" dans la partie "*Accès réseau à distance*" du Poste de travail.

3.- Vérifiez que vous êtes anonyme : Allez sur le site de la CNIL, et regardez si l'adresse IP qui s'affiche est celle attribuée par votre FAI. Pour ce faire, regardez dans l'utilitaire *Winipcfg.exe* dans le répertoire "Windows" de 95/98 ou tapez *ipconfig.exe* dans la fenêtre "d'invité de commandes" sous Windows® 2000, puis comparez à l'adresse qui s'affiche sur le site de la Cnil. Si c'est la même, recommencez la procédure !, vous avez oublié quelque chose... En revanche, si l'IP correspond à celui de votre *proxy* alors vous êtes l'homme invisible !

Explications.- Il existe sur le net des proxies anonymes (sans login ni password) et gratuits où les internautes on la possibilité de s'y connecter dans certaines circonstances. Le *proxy*, comme nous l'avons vu, via notre requête se charge de récupérer la page souhaitée avec son IP qui elle est statique. Donc la votre est invisible.

L'idéal est de chaîner plusieurs *proxies*, de préférences localisés dans des pays différents du votre. Les chances de remonter jusqu'à vous sont quasi-nulles. Sachez toutefois que votre FAI peut très bien regarder ce qui transite sur votre compte, quel que soit le nombre de *proxies* utilisés. Mais vous êtes couvert dans la mesure où votre compte est bidon et vous cachez votre numéro de téléphone (vous me suivez ?).
Par-contre si une instruction judiciaire est ouverte à votre encontre, alors votre FAI peut "unshadower" votre numéro de téléphone à l'aide de *France Télécom* pour remonter jusqu'à vous.

De plus, les *proxies* peuvent vous identifier car ils loguent (génèrent un fichier d'information) vos connexions, d'où la nécessité de les chaîner.

Quelques bons proxies anonymes

URL	Port	Date de test
alpha.cosapidata.com.pe	80	19.08.2000
cache1.cc.interlog.com	3128	19.08.2000
proxy.cybergate.co.zw	8080	19.08.2000
proxy.qatar.net.qa	8080	19.08.2000
sunsite.icm.edu.pl	8080	19.08.2000
zm4.zptc.co.zw	8080	19.08.2000

4.- Les Tunnels

Nous avons vu que malgré l'utilisation de *proxies*, l'anonymat est toute relative car votre fournisseur d'accès Internet (FAI), bien que ne connaissant pas le détail de vos navigations, peut parfaitement intercepter et analyser les données transitant entre votre ordinateur et votre proxy. De plus de tierces personnes peuvent également surveiller vos données en transit sur le réseau.

Un tunnel est une liaison cryptée entre votre ordinateur et le service que vous utilisez comme *proxy*.

Les données que vous enverrez à un service *Proxy* devront être cryptées par vos soins, ce dernier les décryptera et les enverra à leur destinataire. A contrario, les données qui vous seront envoyées en retour, seront cryptées en temps réel par le *proxy* qui vous les enverra. Ces données seront donc illisibles par votre FAI et par toute personne interceptrice.

Les données peuvent concerner des E-mails, des articles de forums de discussion, des adresses Web ou FTP, etc.

Les proxies qui acceptent de crypter/décrypter vos données sont généralement payants comme le « *tunnel* » de anonymizer.com nommé « *Pipeline anonymizer* » ou encore, celui de IDSecure.

Il est nécessaire de se procurer un logiciel, comme le partagiciel Secure CRT, qui cryptera/décryptera vos données, ce dernier doit être le même que celui utilisé par le *proxy*. Il vous faudra le paramètrer (nom ou adresse IP du *Proxy*) et lui indiquer quelles données devront être traitées : E-mails, HTTP, FTP ou newsgroups. Les clés personnelles de cryptage/décryptage vous seront envoyées lors de votre première connexion au *Proxy*.

Enfin, votre client Web, de messagerie ou de groupe de discussion devra être configuré afin qu'il reconnaisse votre « *tunnel* » et y envoie vos requêtes que ce soit pour le Web, vos e-mails ou les Newsgroups.

Comme tout Proxy, vous bénéfierez également du camouflage de votre adresse IP.

5.- Les Firewalls

Les pare-feu sont des outils consacrés à votre défense. C'est une protection logicielle (ou matérielle) qui à pour mission de protéger les échanges de données entre votre machine et le réseau Internet. Son rôle est d'analyser les paquets IP qui circulent entre le réseau et votre ordinateur afin de filtrer le flux de données entrantes et sortantes.

Un micro connecté à l'Internet est vulnérable aux attaques de pirates : visites, vol, destruction de fichiers, introduction de virus ou de code dommageable pour vos données…, car il présente de nombreuses portes ouvertes, appelés ports, que les hackers savent exploiter pour pénétrer votre intimité informatique.

Sachez que votre machine communique avec l'Internet au travers de 65536 Ports de communication et que les ports non utilisés restent ouverts, qui sont autant de portes d'entrées ! Chaque service Internet (ou protocole) à son numéro de port, par exemple HTTP utilise le port 80, FTP le port 21, Telnet le port 23, le courrier expédié (SMTP) utilise le port 25 et celui reçu (POP3) le port 110, etc.

Microsoft a choisi d'ouvrir des ports permettant l'échange de fichiers au sein d'un réseau dans Windows 95/98/NT. Ces ports (par défaut les 137, 138, 139) sont de véritables trous béants pour les hackers qui ne cessent de les exploiter. Steve Gibson décrit une méthode sur son site, permettant de s'assurer que votre port 139 (et accessoirement les 137 et 138) ne restent pas ouverts à la merci d'une éventuelle intrusion.

Le firewall ferme les ports non utilisés et tient à l'œil les applets Java et contrôles ActiveX. Quand un pare-feu détecte une connexion suspecte il affiche une fenêtre d'alerte avec quelques informations dont l'adresse IP de l'intrus, quelques firewalls identifient même le fournisseur d'accès Internet ! (C'est le cas de NetCommando). Lockdown 2000, lui, est capable de détecter un « scan » de votre adresse IP et de vous renvoyer l'adresse IP de l'auteur de la recherche ! (une version de l'arroseur arrosé).

Notez au passage qu'il est possible d'identifier la machine d'un intrus à partir de son numéro IP, grâce à la base d'interrogation WHOIS (http://www.ripe.net/cgi-bin/whois).

Je vous recommande vivement de mettre en place un firewall simple à configurer (beaucoup sont complexes), comme l'excellent *ZoneAlarm* qui à la particularité d'être gratuit et accessible aux novices !
Vous trouverez toutes les infos en français sur tous les firewalls sur le site Firewall.net.

En dehors des intrusions, il assurera également la surveillance des informations émises par les espiogiciels (ou spyware), ces petits utilitaires (ou grandes applications) qui se connectent à l'Internet afin d'envoyer des informations personnelles à votre insu.
Après avoir bloqué la connection, *ZoneAlarm* vous permettra d'accepter ou de refuser (définitivement ou ponctuellement) tout accès Internet et ce , pour chaque application !

Le site de *Steve Gibson* permet de tester en ligne la sécurité de sa connection Internet ainsi que tous vos ports ouverts en allant dans la section ShieldsUP! et en sélectionnant au choix le menu « **Test my Shield »** (tester mon bouclier) ou « **Probe my Ports** » (scanner mes Ports). Un compte rendu très explicite est généré avec des recommandations (malheureusement en Anglais).

Je vous conseille de faire le test avant l'installation d'un fireWall et après. En ce qui me concerne, les ports préalablement ouverts dont le 139 étaient tous fermés et la sécurité parfaitement assurée après l'installation par défaut de *ZoneAlarm*.

Enfin, petite précision qui a son importance sur la configuration réseau de votre machine. Allez dans les « propriétés réseau » et supprimez tous les protocoles autres que TCP/IP si votre machine n'est pas en réseau.
Tout le reste doit être supprimé car ils aggravent la vulnérabilité de votre PC en matière d'intrusion. S'agissant d'IPX/SPX, il est vrai que ceux d'entre vous qui jouent à des jeux nécessitant ce protocole, il vous faudra le conserver.

B.- La Messagerie Electronique.

1.- Les Remailers.

Vous pouvez souhaiter envoyer un courrier de façon anonyme c'est à dire sans divulguer votre identité au destinataire. Bien sur vous pouvez modifier votre adresse e-mail dans votre navigateur mais l'en-tête de votre courrier comporte de nombreuses informations dans son en-tête, dont votre adresse IP.

Comme nous l'avons vu ci-dessus, à partir de votre adresse IP les bases d'interrogation spécialisées peuvent divulguer votre identité ou celle de votre fournisseur d'accès (qui enregistre vos connexions dans ses fichiers *log*).

De plus, votre fournisseur d'accès Internet (FAI) peut lire votre courrier, il convient donc, pour une plus grande confidentialité, en plus de cacher votre adresse IP, de crypter vos messages entrants et sortants.

C'est le rôle dévolu aux *remailers* ou *ré-achemineurs*, qui cryptent votre courrier sortant tout en dissimulant les informations pouvant vous identifier, dont votre adresse IP.
Un ré-acheminеur, digne de ce nom, ne connaît pas votre adresse e-mail réelle.

La procédure a suivre est d'indiquer au *remaile*r l'adressse de votre correspondant qui peut être un autre *remailer* ! vous pouvez chaîner autant de *remailers* que vous le souhaitez, et je vous le recommande vivement pour deux raisons :

- Le dernier *remailer* de la chaîne ne saura pas d'ou vient le message.

- En cas de contrôle par les services de police, il suffit que l'un d'eux ne soit pas contrôlé pour que votre message soit confidentiel.

Sachez toutefois que le risque de perte de votre message est proportionnel au nombre de *remailers* et que plus il y a « d'intermédiaire » plus votre message sera long à arriver à son destinataire. De plus si un des *remailers* n'est plus en activité votre message est perdu, d'où la nécessité d'un suivi accru.

Il existe une cinquantaine de *remailers* de par le monde scindés en deux familles : les *Cypherpunks* et les *Mixmaster*.
Ces derniers découpent vos messages en morceaux de 29Ko, rendant la surveillance des messages plus difficile et le niveau de sécurité s'en trouve accru par rapport aux premiers.
Le plus connu est certainement Anonymizer, citons aussi AnonMailNet et MailAnon.

Certains *remailers* n'acceptent que les messages cryptés à l'aide de *PGP* (Pretty Good Privacy) et rejettent tout autre message. Dans ce cas vous pouvez utiliser *Private Idaho*

ou *Jack B. Nymble* (*JBN)* qui automatise le travail d'encryption et tient une liste de *remailers* à jour (très important) de plus, la procédure de composition des messages, très strict, est automatisée.

Vous trouverez une liste de *remailers* à jour à l'adresse :

http://www.cs.berkeley.edu/~raph/remailer-list.html

Ou sur le site du *Centre d'Information pour l'Anonymat Electronique* (Epic) qui maintient à jour une liste de ré-acheminеurs fiables.

La réception anonyme de courriers électroniques est finalement plus problèmatique car les *remailers* ne le permettent pas et les messageries gratuites, malgré le fait de pouvoir entrer de fausses informations nominatives, offrent très peu de possibilité d'anonymat du faît qu'elles mémorisent souvent votre adresse IP ou qu'elles vous obligent à accepter un *cookie*. Les *proxies* peuvent être une solution partielle mais les *Nymservers* vous garantissent l'anonymat absolu…

2.- Les Serveurs de pseudonymes.

Un *nymserver* est un serveur de mail auprès duquel vous ouvrez un compte, comme tout serveur de mail, à la différence duquel le courrier envoyé indiquera comme expéditeur le suffixe <votre_email**@ServerNym**> en lieu et place du nom de votre fournisseur d'accès.

De plus le courrier reçu sera automatiquement réexpédié vers une compte e-mail ou un forum de discussion public sous forme crypté (vous seul saurez le décrypter) , sans que le *nymserver* puisse savoir qui le recevra en bout de chaine.

L'avantage du forum de discussion pour recevoir votre courrier c'est que vous n'êtes pas obligé d'avoir un compte chez un prestataire auprès duquel il faudrait vous identifier.

Allez voir sur « *alt.privacy.anon-messages* », afin de voir à quoi ressemble un message émis par un *nymserver*.

Au moment de la création de votre compte, envoyez un e-mail vide au nymserver de votre choix (list@nymserver), vous recevrez en retour une liste des noms déjà utilisés sur ce nymserveur.

Utilisez le logiciel *JBN* (voir la section sur les *remailers*) pour créer, paramètrer et maintenir votre compte. Il vous faudra préalablement bien comprendre le principe des *remailers* et plus particulièrement des chaines de *remailers* avant de vous attaquer aux *nymservers* car ils sont utilisés pour définir le chemin que devront prendre les messages pour vous parvenir (*Reply Blocks)*.

Il existe actuellement 3 *nymservers* :

- nym.alias.net
- redneck.gacracker.org
- anon.xg.nu

Recevoir un message sur un compte *nym* peut prendre plusieurs heures contrairement à un e-mail classique mais c'est la contrepartie de la garantie d'un anonymat absolu pour un compte *nym* bien configuré.

3.- Les Certificats de sécurité.

Les identifications numériques (également appelées certificats) ont deux rôles :

1- S'assurer de l'identité de l'expéditeur d'un message ou d'une transaction électronique (pour le cas d'un site Web) de la même manière que vous présentez votre carte d'identité à une administration. Elle assure l'authenticité des documents envoyés et qu'ils ne sont en aucune manière interceptés ou lus par des personnes autres que leur destinataire d'origine.

2- Cette identification numérique peut aussi vous servir à crypter des messages (et leurs pièces jointes) pour les rendre inviolables. Pour ce faire, ils intègrent la norme S/MIME pour le courrier électronique sécurisé.

Le format de normalisation est le X509. Il s'agit du format le plus utilisé dans les navigateurs Web pour sécuriser le transfert des pages Web. Les certificats X509 sont analogues à une signature PGP. Ainsi vous pouvez même les demander pour votre clé PGP existante (voir la section sur la *cryptographie*).

Un identificateur numérique inclus une "clé publique", une "clé privée" et une signature numérique. *La combinaison signature numérique + "clé publique" est appelée "certificat"*.

Les destinataires de vos messages peuvent :

- Utiliser votre signature numérique pour vérifier votre identité.

- Utiliser votre "clé publique" pour vous envoyez des messages cryptés.

De votre côté (en tant que destinataire) :

- Utilisez votre "clé privée" pour décrypter vos messages cryptés et les lire en clair.

- Utilisez la "clé publique" de vos destinataires pour leur envoyer des messages cryptés. (attention, dans ce cas il est indispensable votre carnet d'adresses contienne les identifications numériques de vos destinataires).

Avant de pouvoir envoyer un message signé numériquement, vous devez vous procurer une identification numérique (voir ci-dessous). Si vous envoyez des messages cryptés, l'identification numérique de tous les destinataires de ce message doivent être enregistrées dans votre carnet d'adresses.

Les identifications numériques sont délivrées par des autorités de certifications indépendantes (*Verisign*, *GlobalSign*, *American Express*, etc.) qui contrôlent votre identité avant d'émettre l'identification. Leur coût est d'environ 60 FF le certificat (variable selon l'autorité), mais le site Web Thawte dans le cadre de son offre Freemail, propose gratuitement des certificats au format S/MIME, PGP et SSL.

Pour *Outlook* et *Outlook Express*, en dehors de *PGP*, il existe une autre possibilité interne au programme. Si un de vos correspondant vous a déjà envoyé un message crypté, vous disposez de sa signature numérique et vous pouvez donc, vous aussi, lui envoyer un message protégé en cliquant sur l'icône "*Crypter*" de la fenêtre de message.
Sinon, vous pouvez vous procurer un certificat numérique en suivant la démarche ci-dessous :

Sélectionnez "*Outils*", "*Options*", puis cliquez sur l'onglet "*Sécurité"*. Choisissez la case "*Obtenir une identification numérique*".

Netscape Messenger propose uniquement un module *S/MIME* désactivé par défaut. Le cryptage se fait alors en mode *SSL*. Il vous faut obtenir un certificat numérique :
Sélectionnez le menu "*Communicator*", sous-menu "*Outils"*, "*Informations sur la sécurité"*. Cliquez sur le lien "*Vos certificats"* dans la colonne de gauche de la boîte de dialogue qui s'affiche. Cliquez ensuite sur le bouton "*Retirer un certificat"*.
Lorsque vous écrivez un message, cliquez sur l'onglet "*Options"* de votre fenêtre de message puis sélectionnez la case "*Chiffré"*.

Pour coder un message avec *AOL*, utilisez le plug-in *PowerMail* developpé par *BPS Software*. Il coûte environ une centaine de francs avec une version gratuite pour vos correspondants, afin qu'ils puissent déchiffrer vos messages.

4.- La Cryptographie.

La cryptographie avec PGP

La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelé le *cryptage*. La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage des données.

Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés tel que l'Internet, afin qu'aucune personne autre que le destinataire ne puisse les lire.

Le chiffrement fait appel à deux techniques, le *cryptage symétrique* (une seule clé pour chiffrer et déchiffrer) et le *cryptage asymétrique* qui utilise une *clé publique* non protégée qui chiffre mais ne déchiffre pas et une *clé privée* (jamais transmise et protégée) pour déchiffrer. *PGP* (*Pretty Good Privacy* traduisez par « relativement bonne protection » !), créé par l'américain *Phil Zimmerman* (devenu un mythe*)*, combine les deux méthodes.

Nous allons étudier le principe de fonctionnement de *PGP* Freeware et son installation, fort simple rassurez vous. Pourquoi *PGP* ? sachez que c'est la référence absolue en terme de chiffrement fort comme en terme de confidentialité et d'authentification.

PGP est la solution de cryptographie la plus *invulnérable* capable d'empêcher les gouvernements les plus puissants de lire vos fichiers. A ce jour, même la *NSA*, l'agence de renseignement américaine, malgré ses supercalculateurs et ses cryptanalystes, n'a pas réussi à casser les clés de *PGP* !

De plus, ce produit est disponible sur toutes les plateformes matérielles et tous les systèmes d'exploitations (Windows, Mac, Linux, Unix, OS/2, BeOS), même alternatifs ou ludiques (Atari, Amiga, etc). C'est un produit réellement universel.

Il existe plusieurs utilitaires utilisant la technologie *PGP* :

- Le freeware comporte deux modules **PGPKeys** pour la gestion des clés et **PGPtools** pour le chiffrement, le déchiffrement, la signature et l'effacement.

- **PGPdisk** sert au cryptage des données de tout ou partie d'un disque dur. Il n'est malheureusement plus disponible dans la version freeware, mais dans la version payante. Il permet de créer un volume *PGPdisk* qui, une fois « monté » permet d'être utilisé comme un disque dur externe. On peut y installer des applications et stocker des fichiers protégés par un mot de passe complexe secret.

- **PGPnet** permet la mise en œuvre d'un réseau local dont les communications TCP/IP sont sécurisées entre les postes où PGPnet est installé.

- Des Plug-ins existent pour la plupart des clients de messagerie afin de crypter simplement ses e-mails ou ses pièces jointes : Outlook, Outlook Express, Eudora et Lotus Notes.

- La version payante de *NAI* (Network Associates, la société qui distribue *PGP*) inclus des fonctions comme **l'auto-décryptage** qui permet de convertir des fichiers ou des dossiers en archive d'auto-décryptage pouvant être envoyée à des utilisateurs ne possédant pas *PGP*.

La procédure de cryptage PGP

Avant de crypter un message, celui-ci est comprimé par *PGP* pour limiter la durée de transmission et renforcer la sécurité cryptographique. Puis le programme créer une **clé de cession** aléatoire qui sert à chiffrer notre texte. Ce nombre aléatoire est généré à partir de la frappe sur le clavier et des déplacements de la souris puis un traitement algorithmique lui est appliqué pour le rendre unique. Une fois générée, la *clé de cession* est codée avec la *clé publique* du destinataire du message. Ce destinataire va recevoir en plus du message chiffré, la clé de cession cryptée (avec sa propre *clé publique*).

La procédure de décryptage PGP

Lors de la réception du message crypté, le destinataire se sert de sa *clé privée* pour récupérer la *clé de cession* aléatoire utilisée pour coder le message. Puisque l'expéditeur du message à créé la *clé de cession* (en fait la clé de cryptage) avec la *clef publique* du destinataire, ce dernier peut parfaitement la reconstituer à l'aide de sa *clé privée* car les clés fonctionnent par paires. Une fois en possesion de la clé de cession aléatoire, il ne lui reste plus qu'à déchiffrer le message qui lui a été adressé.

Notez que le mode de cryptage asymétrique s'applique en fait, à la *clé de cession,* qui est de 128-bit, et non au texte lui-même qui subit un cryptage de type conventionnel, ce qui permet un gain de temps considérable.

Comment l'expéditeur peut-il entrer en possession de la clé publique du destinataire ?

- La *clef publique* générée par PGPkey, peut être envoyée soit par e-mail, dans le corps du message ou en tant que pièce jointe, soit sur un serveur de clés publiques (comme pgpkeys.mit.edu) ou d'entreprise, qui stocke les *clés publiques* de nombreux utilisateurs de *PGP*. Il faut récupérer la *clé publique* de la personne à laquelle vous voulez envoyer un message chiffré. Pour cela il faut vous constituer un « trousseau de clés publiques » comprenant les *clés publiques* authentifiées de vos interlocuteurs.

- Vous trouverez notre *clé publique* dans la rubrique « Contact » de notre page d'accueil.

Comment être sur que la clé publique est bien celle de son propriétaire supposé ?

- Comparez l'empreinte digitale numérique (*fingerprint*) de la copie de la *clé publique* sur votre machine avec celle de la clé d'origine. Cette empreinte est constituée d'une liste de mots générés aléatoiremet par l'utilisateur et phonétiquement distincts pour être facilement compréhensible. En comparant cette liste de mots entre la copie de la clé et une disquette remise en main propre, il est possible d'authentifier le détenteur de la clé. Il est également possible de faire lire, au téléphone, l'empreinte digitale de sa clé par le détenteur de la *clé publique*.

Si vous êtes certain de posséder une copie valide de la *clé publique* d'un utilisateur, vous pouvez signer cette clé avec votre *clé privée*. Par cette action vous affirmez votre certitude que la clé appartient bien à son utilisateur présumé. Vous pouvez ensuite exporter cette clé vers un serveur de clés publiques, ce qui renforcera sa crédibilité auprès des autres utilisateurs.

Comment peut-on être sûr de l'intégrité d'un document ?

- *PGP* utilise un procédé d'authentification qui empêche la récupération de la signature d'un document pour la joindre à un autre document. Le message est transformé en un court résumé de 160 bits par une fonction de hachage. Toute modification du message transforme ce résumé qui est ensuite chiffré avec la *clé privée* de l'expéditeur. Le texte en clair et sa signature cryptée sont envoyés au destinataire du message. Ce dernier utilise la *clé publique* de l'expéditeur du message pour vérifier si la signature est correcte.

Installation de PGP freeware

Téléchargez la version française internationnale de PGP freeware à l'adresse suivante :

Site FTP : ftp://ftp.pgpi.org/pub/pgp/6.5/

Site Web : http://www.pgpi.com/

ou sur l'un des nombreux sites Web qui le propose en téléchargement (voir notre rubrique « téléchargement »).

Une fois installée (16Mo), la première étape consiste à créer la *clé publique* et la *clé privée*.
Pour ce faire, lancez le module *PGPkeys* puis suivez les conseils de l' « Assistant de génération de clés ». Nous vous conseillons de ne pas toucher aux options de réglage par défaut concernant le choix de l'algorithme et la taille des clés (2048 bits par défaut).

A noter : la loi française du 17 mars 1999, qui autorise les clés d'une longueur comprise entre 40-bit et 128-bit s'applique à la clé de cession aléatoire, qui chiffre les documents, et non pas aux clés publiques et privées qui comprennent au minimum 1024-bit.

Vous pouvez définir une date d'expiration pour votre clé publique (illimitée par défaut), mais vous ne pourrez plus revenir sur votre choix.

Ensuite, saisissez votre phrase clé complexe (*passphrase*) qui protège votre clé secrète. Utilisez de 20 à 25 caractères au minimum, facilement mémorisables sous forme de mots familiers, de maxime ou de proverbe, par exemple. Evitez de noter cette phrase. Elle vous sera demandée à chaque utilisation de votre *clé privée*, lors de l'envoi et de la réception des messages cryptés.

Votre clé privée secrète est stockée dans le fichier ***secring.pkr****, et votre trousseau de clés publiques est stocké dans le fichier* ***pubring.pkr****, sauvegardez bien ces fichiers !*
Car si quelqu'un recopie votre clé privée, il ne lui manque plus que la phrase de passe (*passphrase*) pour déchiffrer les documents qui vous sont destinés.

Vous pouvez maintenant diffuser votre *clé publique* (et seulement celle là !) afin qu'elle soit utilisée par toutes les personnes désireuses de communiquer avec vous. Pour l'insérer dans le corps d'un message ou en tant que pièce jointe, lancer le module *PGPKeys*, sélectionnez votre *clé publique*, puis cliquez sur *Exporter* dans le menu *Clés*.

Entrez un nom de fichier et sélectionnez un dossier de destination. Votre *clé publique* étant simplement un bloc de texte il est aisé de l'échanger par un copier-coller vers votre client e-mail ou de l'insérer dans votre message en tant que pièce jointe.

Pour la publier sur un serveur de clés (voir plus haut) afin de la rendre accessible au plus grand nombre, connectez-vous à Internet, et laissez vous guider par l' « Assistant de génération de clés » qui vous proposent une liste de serveurs. Cochez la case « *Envoyer ma clé maintenant sur un serveur de clés* ». Il est impossible de supprimer une clé d'un serveur après envoi.

Une fois obtenu la *clé publique* de votre correspondant vous pouvez crypter et envoyer un message à son intention, directement dans votre client de messagerie, si il supporte les Plug-ins *PGP* (principalement *Outlook* et *Eudora*).

Le plug-in *PGP* pour les messageries.

Le plug-in *PGP* intègre directement les fonctions de *PGP* dans l'interface de messageries lors de la procédure d'installation. Sélectionnez le plug-in correspondant à votre messagerie et déselectionnez bien les autres, un risque de bloquage du système pourrait survenir. Ne confondez pas *OutLook* et *Outlook Express*.

Lors de l'envoi d'un message à un ou plusieurs destinataires, les messages en clairs seront directement cryptés par *PGP* avant d'être expédiés. Chaque message est crypté avec la *clé publique* du destinataire reconnu automatiquement par *PGP* à l'aide de l'adresse de messagerie.

Pour pouvoir relire les messages que vous avez envoyé, il est indispensable de se mettre en copie du message original c'est à dire de s'envoyer une copie du message ! Votre copie sera cryptée automatiquent avec votre *clé publique* vous pourrez donc relire le message avec votre clé privée et aucune tierce personnne ne pourra le consulter.

La lecture d'un message chiffré avec votre clé publique peut être réalisée de manière automatique avec le bouton de déchiffrement. La phrase clé (*passphrase*) vous sera demandée et le message apparaîtra en clair sur votre écran.

Enfin, pour éviter la saisie trop fréquente de la phrase clé, il est possible de la mémoriser dans un cache pendant une période prédéfinie (menu *Edit* de **PGPkeys**).

Cryptographie : l'algorithme RSA.

L'algorithme RSA fut inventée par trois scientifiques du MIT : Ronald Rivest (R), Adi Shamir (S) et Leonard Adleman (A) à la fin des années 70. En 1983, ils la brevetèrent comme procédé de chiffrement à clé publique, sans se douter qu'elle deviendrait la base des transactions sur Internet.

RSA se retrouve aujourd'hui universellement utilisé pour les échanges sécurisés, mais constitue surtout la pierre angulaire des opérations de chiffrement et d'authentification sur Internet dans les protocoles S/MIME (messagerie électronique sécurisée), SSL (*Secure Socket Layer* pour les transactions chiffrées) ou S/WAN (système d'échanges Internet protégés).

Elle est intégrée dans les principaux navigateurs Internet pour permettre les transactions sécurisées et quelques services de messageries en lignes (comme ZipLip) l'utilise pour sécuriser leurs messages par chiffrement via SSL ou S/MIME. A ce propos, nous vous recommandons d'utiliser les versions 128-bit de vos navigateurs, qui bénéficierons d'une bien meilleure protection cryptographique pour les services sécurisés en ligne.

Allez dans la boîte de dialogue Aide | A Propos d'Internet Explorer. Regardez la ligne nommée « Puissance de chiffrement » qui indique le niveau de cryptographie actuelle (par défaut 40-bit). Si ce niveau est inférieur a 128-bit allez sur le site de Microsoft ou de Netscape pour télécharger la version ou le patch « high encryption128-bit » disponible pour Windows, Windows 2000 et Mac (également sur notre CD-ROM).

Aujourd'hui que le brevet RSA est tombé dans le domaine public, chacun peut désormais l'intégrer à ses logiciels sans devoir payer de droits.

La Stéganographie

C'est une technique de cryptographie qui consiste à insérer (fusionner) un fichier quelconque dans un second fichier (image, son Wav, page HTML, etc.) sans que l'aspect extérieur de ce dernier ne soit modifié, hormis sa taille.

Le camouflage est parfait et le fichier, d'apparence ordinaire, peut passer tous les réseaux d'espionnage comme Echelon, sans être inquiété.

Le meilleur programme de ce genre est certainement Invisible Secrets Pro qui dispose même d'un petit « Reader » gratuit qui permet à votre destinataire d'extraire vos messages sans posséder le programme complet (voir notre section « outils »).

5.- Les messageries anonymes

Sur l'Internet il existe de nombreux sites, souvent gratuits, qui proposent d'envoyer des e-mails de façon plus ou moins anonyme au travers d'une interface de type « Webmail » ou quelquefois un *applet* Java. C'est une solution qui à le mérite de la simplicité, l'utilisation de *remailers* éventuels étant transparente pour l'utilisateur final.

Citons le site français SiteFacile, le site miroir français de Anonymizer ou encore le site ZipLip qui crypte vos e-mails avec le protocole sécurisé *SSL*. Vous trouverez une liste exhaustive détaillée dans la rubrique « annuaire des sites d'anonymat » sur notre site.

Certains sites imposent un formulaire d'enregistrement, d'autres sont en entrée libre. Préférez les seconds.

Des logiciels d'anonymat sous Windows ou Dos permettent d' « anonymizer » vos messages voire pour certains d'en personnaliser les en-têtes. Ils peuvent utiliser ou non des *remailers*. Ces « anonymous e-mailers » sont très peu nombreux et difficiles à débusquer dû à leur caractère « underground ».

Citons *GhostMail* qui sous une interface sympathique, permet, en plus des e-mails, de poster des messages anonymes sur les groupes de discussions.

Vous trouverez une liste de quelques logiciels de messagerie anonyme dans notre rubrique « *Outils* », à utiliser avec précautions.

6.- Les réseaux d'espionnage d'Etat – Echelon.

Peut-on envoyer un e-mail en étant certain de n'être pas intercepté par les grandes oreilles électroniques des réseaux d'espionnage tels que *Echelon* ?

Rappelons que le réseau américain *Echelon* intercepte toutes les commnunications (et pas seulement les e-mails) à partir de mots clés dits « sensibles » et dont vous trouverez une liste (au format A*crobat* pour éviter les référencements) dans notre dossier sur *Echelon*.

Il est prétentieux de prétendre passer au travers d'un tel système, de par son envergure et les moyens monumentaux mis en œuvre, cependant je vais tenter de vous proposer quelques solutions.

- Le cryptage avec *PGP* est la solution la plus connue pour protéger ses correspondances de la curiosité des gouvernements (voir la section sur *PGP*). La clé semble résister aux supercalculateurs de la *NSA* mais pour combien de temps encore ? et en est-on vraiment certains ?

- La *Stéganographie* est une technique de cryptographie qui permet de camoufler un fichier quelconque (MP3, texte, page HTML) dans une image, de façon invisible. Cette technique est redoutable d'efficacité d'autant que le document peut-être préalablement crypté avec *PGP*.

- Puisque *Echelon* cherche des mots clés, pourquoi ne pas écrire son courrier dans un logiciel de dessin ? en générant un fichier graphique contenant le texte en clair, mais indétectable sauf à passer chaque image à l'O.C.R. (dans ce cas on utilisera une police fantaisie et un format de fichier peu courant). Aucun mot clé « sensible » ne sera détecté par Echelon !

C.- Les groupes de discussions.

Poster un message dans un *Newsgroup* n'est pas aussi anonyme qu'on le croit : tout à chacun, assez proche de vous pour simplement connaître votre nom, peut vous surveiller !

Des moteurs de recherche spécialisés traquent les messages comme Dejanews, outil redoutable s'il en est, ce service indexe le contenu de quatre-vingt mille forums de discussions depuis cinq ans, par nom, e-mail, auteur et sujet.

On serait alors tenté de modifier simplement son nom par un pseudonyme et son adresse E-mail par une adresse gratuite, dans les préférences de son navigateur préféré. Cela sera certainement suffisant pour éviter le repérage dans *Dejanews* mais certainement pas pour assurer votre anonymat : la plupart des serveurs de news enregistrent et transmettent votre adresse IP qui est affichée dans l'en-tête du message posté !

Poster un message anonyme, requière la même démarche que pour les e-mails, vous pouvez soit :

- Passer par un site Web qui prend en charge l'anonymat du message posté en se faisant passer pour l'expéditeur à votre place.

- Passer par un logiciel spécialisé dans l'anonymat comme *GhostMail* qui « anonymize » les informations présentes dans le message.

- Poster votre message à travers une chaîne de *remailers*, comme pour les e-mails anonymes. Votre IP ne sera pas indiquée mais les forums français n'apprécieront pas et vous risqueriez d'être censuré ! (vive la démocratie)

- Passer par un serveur « *Proxy Socks* » pour vous connecter a un serveur de news. Ce sera l'adresse IP du *socks* qui sera affichée dans vos messages. Mieux, chaînez 2 ou 3 *Socks* ! Anonymat garantie.

Qu'est-ce un Proxy Socks ?

Egalement appelés « *Socks* », ces proxies particuliers permettent de relayer une requête NNTP ou FTP/IRC afin de se connecter à votre place selon le même principe que les proxies « normaux ».
Les *Socks* (type 4 ou 5) sont des *proxies* particuliers qui utilisent le **port 1080**.

Pour déclarer votre *Proxy Socks* utilisez le programme gratuit SocksCaps (ou ftp://ftp.nec.com/pub/socks/) si le logiciel de news ne prévoit pas cette possibilité, mais n'indiquez pas un *Socks* dans la zone réservée aux Proxies de votre navigateur !

Les logiciels de News comme *Agent* ou « *Free Agent* », sa version gratuite, ou *Gravity* fonctionnent parfaitement lorqu'ils sont exécutés à travers *SockCaps*, votre adresse IP est alors celle du *Socks*, s'il est situé en Thaïlande, ce sera une adresse IP Thaïlandaise !

Cependant , bien que votre adresse IP soit celle du *Socks*, le path indiquera votre fournisseur de news (news.monfai.fr par exemple). L'idéal est alors d'utiliser un serveur de News « ouvert » afin de poster vos messages dans les groupes qui vous interressent. Le logiciel News Hunters vous permet de trouver les serveurs « ouverts » en écriture en testant tous les serveurs de news de tous les participants d'un forum, il fonctionne dans 20% des cas, ce n'est déjà pas si mal.

D.- Les messageries en direct.

Ils constituent ce que l'on appelle les « *Chat* » (bavardage) ou *IRC* (Internet Relay Chat). Ce réseau est très peu sécurisé et les données transitent en clair et sont donc parfaitement lisibles.
Les plus connus sont *Microsoft-Chat, Mirc* et *AOL ICQ* (racheté à la société israèlienne Mirabilis).

Sachez qu'il n'est pas aisé d'être anonyme sous ces services : votre adresse IP est facilement accessible et est toujours disponible sous *ICQ*.

Deux solutions s'offrent à vous :

- Utiliser un « *Proxy Socks* ».
- Utiliser un service d'anonymat qui supporte le protocole IRC.

Qu'est-ce un Proxy Socks ?

Nous avons vue le rôle d'un proxy « normal » : se connecter sur un serveur (Web ou parfois FTP) au nom du client (vous) puis vous retransmettre les données. Pour le serveur d'application le serveur *proxy* est le client, vous êtes donc inexistant donc anonyme.

Egalement appelés « *Socks* », ces proxies particuliers permettent de relayer une requête lancée par *ICQ* ou par un logiciel IRC/FTP/Telnet afin de se connecter à votre place
Les *Socks* (type 4 ou 5) sont des *proxies* particuliers qui utilisent le **port 1080**.

Pour déclarer votre *Proxy Socks* utilisez le programme gratuit SocksCaps (ou sur ftp://ftp.nec.com/pub/socks/) si le logiciel ne prévoit pas cette possibilité. Lancez votre logiciel à travers *SocksCap,* l'adresse IP visible sera celle du *Socks*, s'il est situé en Thaïlande ce sera une adresse IP Thaïlandaise !

Les services d'anonymat sous IRC

Il existe très peu de solutions spécialisées d'anonymat qui supportent le protocole *IRC*, citons l'excellent Freedom (voir notre « *annuaire* » des services d'anonymat et notre article sur *Freedom* dans les « *archives »*), qui propose contre un abonnement raisonnable, un anonymat absolu sur ces canaux *IRC* (entre autre) également le programme Ultimate Anonymity (voir plus bas).

Concernant *ICQ*, sachez qu'il intègre un mouchard ! celui–ci ferait l'inventaire de vos programmes et numéros de séries associés avant de renvoyer le tout aux serveurs d'*ICQ*.

Voici comment désactiver ce mouchard :

Lancez Regedit (Démarrer|Exécuter), l'éditeur de la base de registre.

Placez vous sur **HKEY_CURRENT_USER / Software / Mirabilis / ICQ / Defaultprefs**

Trouvez la clef « **Auto Update** » et changez la valeur de 'Yes' en '**No**'.

Félicitations, vous venez de terrasser votre premier mouchard !

Enfin, si vous ne vous sentez pas de taille à affronter la base de registration de Windows, vous pouvez utiliser un utilitaire qui fera le travail tout seul. Citons pas exemple l'excellent *Hulk Maximizer* qui, sous l'onglet « Mouchards », cache une arme redoutable qui supprimera également le mouchard de Windows 98 !

Les messageries communautaires

Le concept de partage de fichiers distribués a donné naissance à toute une gamme de messageries instantanées basées sur un système d'échange horizontaux, ayant pour point commun une architecture poste à poste (point par point), brouillant la distinction entre client et serveur pour d'avantage d'anonymat.

Napster, développé par un jeune étudiant en informatique de 19 ans, Shawn Fanning, a initié l'ère d'un nouveau type de messagerie communautaire ou , tout à chacun peut partager tout ou partie de son disque dur afin de mettre à disposition son catalogue de fichiers MP3. Malheureusement son modèle, basé sur un serveur central unique est fragile et son avenir, mis à mal par les coups de boutoir des *Majors* de l'industrie du disque, est pour le moins incertain.

Gnutella, produit « *open source* », reprend ce principe mais l'étend à tous les types de fichiers et supprime ce concept de serveur central, talon d'achille du système. Chaque station connectée est à la fois serveur et client. Il diffuse la recherche à l'ensemble des serveurs du réseau, passant la requête de machine en machine, celle qui a le fichier désiré l'envoie au suivant empruntant le chemin inverse et le téléchargement peut débuter. Gnutella fonctionne sur tous les systèmes d'exploitation.

Imaginé par un jeune programmeur irlandais Freenet a demandé plus de deux années de développements. Son protocole **garantie un anonymat complet** aussi bien de l'émetteur d'information que des lecteurs : la requête circule (et est réitérée) de nœud en nœud jusqu'à avoir décelé le document demandé mais on ne peut pas retrouver qui est le demandeur d'origine, ni le vrai serveur.

Son architecture est elle que toute censure y est impossible : tout document demandé est aussitôt reproduit sur tous les ordinateurs participant au réseau ! De plus il intègre un processus qui réduit les risques de contrôle.

Sur *Freenet* chaque serveur possède une partie de l'index listant tous les fichiers disponibles. Chaque fichier est découpé en huit parties qui empruntent des chemins différents et se répliquent en fonction de la demande ; il suffit d'en récupérer quatre pour reconstituer le document !.

Freenet, comme *Gnutella,* est un logiciel libre au code source disponible, ce qui le met à l'abri d'éventuels *mouchards* ou *backdoors*.

E.- Les services d'anonymat Mixtes.

Une nouvelle catégorie de services redoutablement efficaces viennent d'apparaître. Ils associent une application tournant en tâche de fond à un proxy en ligne.

Citons les deux principaux : Freedom de Zero Knowledge et PrivadaProxy que vous trouverez dans notre section « Annuaire » sur notre site Web.

Freedom est un cas à part car c'est le plus complet des services d'anonymat. Il étend ses capacités à presque tous les protocoles Internet : navigation Web, messageries : E-mail et Chat, Usenet (groupes de discussions) et Telnet à l'exception remarquable de FTP.

Il utilise des algorithmes de chiffrement « fort » basé sur un système de cryptage asymétrique avec une clé publique (voir section sur *PGP*).

Comme aucune information nominative n'est demandé à l'inscription, l'auteur n'hésite pas à se dire dans l'impossibilité de lever le voile sur l'identité de ses clients !

Mais ne vous croyez pas soumis à l'impunité : un comportement illégal peut entrainer la résiliation de votre compte, même si celui-ci reste anonyme.

Enfin, si vous ne vous sentez pas de taille à gérer les proxies, socks et autres remailers, un programme Ultimate Anonymity vous donne accès à toute la panoplie : E-mails, surf, newsgroups, ICQ/IRC et Web-Chat entièrement anonymes ! il vous en coûtera 19$ (contre la gratuité pour nos méthodes), mais plus vous n'aurez pas le choix des proxies, remailers et socks utilisés.

F.- Conclusion.

J'espère que ce tour d'horizon sur l'anonymat, vous aura permis d'apprendre beaucoup de choses nouvelles. Sachez que ce dossier est mis à jour au fur et à mesure des informations qui entrent en ma possession. N'hésitez pas à me faire part d'éventuelles erreurs, de précisions utiles, de nouveaux sites ou services et surtout enrichissez-le de votre expérience.

J'espère que ce dossier ne sera pas utilisé à mauvais escient, mais uniquement pour protéger votre droit à la vie privée.

Vous trouverez tous les utilitaires décrits dans ce dossier et sur notre site (et bien plus) sur notre CD-ROM remis à jour périodiquement. Contactez-nous.

Enfin, selon la formule consacrée, « *je décline toute responsabilité, de quelques natures qu'elles soient, quand à l'utilisation qui sera faite des services, techniques et méthodes décrites dans ce dossier* ».

Denis Dubois

Webmestre de anonymat.org