

1 L'ANONYMAT SUR INTERNET

1.1. Anonyme sur Internet ?

L'Internet est une gigantesque base de données, accessible à tous. L'une de ses caractéristiques principales est la possibilité pour l'internaute d'être anonyme. A titre d'exemple, le mot le plus entré dans les moteurs de recherche est "sexe". Cela tend à prouver que l'internaute se crée en surfant un personnage virtuel, le nomme (les pseudonymes), et laisse libre court à ses fantasmes. L'impression d'anonymat permet ainsi à de nombreux utilisateurs de rechercher des informations sur les sujets qui les intéressent (même ceux qui sont trop tabous pour être eXprimés dans la vie de tous les jours), ou d'utiliser des chats pour discuter (là encore, la plupart des utilisateurs modifient à des fins plus ou moins honnêtes au moins une de leurs caractéristique (pseudonyme, âge, sexe, ou métier, etc.)). En effet, l'internaute est maître de son destin (il peut se déconnecter quand il veut ou stopper un dialogue sur un chat, etc...). En clair, une croyance (fausse) veut qu'on ne laisse aucune trace pistable sur Internet si on ne le souhaite pas. Erreur, le surf sur Internet est tout sauf anonyme. Que vous souhaitiez être anonyme pour éviter des détournements commerciaux ou protéger votre ordinateur des hackers : " Souriez, vous êtes filmés ! "...

1.2. La preuve...

La C.N.I.L (Commission Nationale de l'Informatique et des Libertés) est l'organisme qui lutte contre l'utilisation abusive de données concernant les internautes français). Pour évaluer votre anonymat sur Internet, rendez-vous sur le site de la **C.N.I.L** : www.cnil.fr

Vous avez là un exemple (simple) de ce qu'un site peut connaître de vous. Admettons maintenant que vous visitiez et passiez une commande sur un site commercial (vous laissez vos coordonnées, votre e-mail, etc.). Ceux-ci vendent la dernière version de votre navigateur Internet préféré (que vous n'avez pas). Si vous n'avez pas coché (et c'est en général bien caché...) que " vous ne souhaitez pas être informé des offres publicitaires du site ", vous recevrez un petit mail vous proposant la dernière version de votre navigateur. L'intérêt commercial est évident dans ce cas-là...Ceci est à simple titre d'exemple.

1.3. L'adresse IP

Tout utilisateur d'Internet utilisant le protocole TCP/IP possède une adresse IP . Un petit exemple :

Lorsque vous vous connectez à notre site, vous entrez l'URL " <http://www.yyyyy.com> ". Ceci est en quelque sorte la version texte de l'adresse IP . Cette adresse cache pourtant une adresse numérique (comme un numéro de téléphone). Si vous entrez " <http://xx.xxx.xx.xxx> " où x est un chiffre, vous arriverez au même endroit.

1.4. L'adresse MAC

L'adresse MAC n'est contrairement à son nom pas réservée aux utilisateurs de Macintosh. Elle signifie Medium Access Control. Celle-ci est fixe pour tous les ordinateurs et accessible par tout le monde. Chaque adresse MAC est également unique au monde. Elle est spécifiée sur votre carte réseau (modem, etc.) lors de sa fabrication. Pas de panique cependant, elle ne peut être eXPloitée que difficilement puisqu'elle ne qualifie qu'un périphérique matériel. Sachez cependant, qu'en cas d'action illégale très grave, il sera possible de remonter jusqu'à vous (par le fabricant de votre matériel, puis par le grossiste, et enfin par le vendeur de votre ordinateur). Elle peut également être utilisée pour vous interdire l'accès à un site par exemple (ce que ne peut pas faire l'adresse IP puisqu'elle est temporaire).

1.5. Connaître votre IP et votre MAC

Pour connaître vos adresses IP et MAC, il vous suffit d'exécuter sur la ligne de commandes la commande: **IPCONFIG /ALL**

Vous obtenez alors un écran de ce type:

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrateur>ipconfig /ALL

Configuration IP de Windows 2000

    Nom de l'hôte . . . . . : mmi
    Suffixe DNS principal . . . . . :
    Type de n_ud . . . . . : Diffuser
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non

Ethernet carte Connexion au réseau local :
    Suffixe DNS spéc. à la connexion . :
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
on
    Adresse physique . . . . . : 00-04-23-07-4B-E9
    DHCP activé . . . . . : Non
    Adresse IP . . . . . : 212.217.79.68
    Masque de sous-réseau . . . . . : 255.255.255.0
    Passerelle par défaut . . . . . : 212.217.79.65
    Serveurs DNS . . . . . : 212.217.0.1
    : 212.217.0.12

C:\Documents and Settings\Administrateur>
```

1.6. Les Proxies : définition et efficacité

La plupart des fournisseurs d'accès utilisent des proxies. Vous avez peut-être déjà remarqué ce terme lorsque vous chargez une page web. Certains sites vous demandent également si vous utilisez un proxy. Un proxy est en fait une barrière filtrante (un serveur) entre vous et le site visité. Le contact n'est en effet pas direct entre vous et le site, mais passe par le serveur proxy du fournisseur d'accès. La démarche est la suivante :

- ☞ vous envoyez une requête au serveur proxy (une adresse de site par exemple)
- ☞ celui-ci envoie la requête au site concerné.
- ☞ le serveur charge alors la page demandée.
- ☞ il vous la transmet ensuite.

Croire que vous êtes alors totalement protégé serait une erreur. Il est bien sûr recommandé d'utiliser un fournisseur possédant un serveur proxy plutôt qu'un fournisseur n'en utilisant pas (qui est donc moins cher la plupart du temps). Le problème est que les serveurs proxy sont tous différents selon votre fournisseur d'accès. L'échelle de la barrière filtrante (rôle joué par le proxy) va du filtre nul (ou presque) au filtre important. Certains serveurs proxy laissent passer la plupart des informations vous concernant (et envoient tel quel vos requêtes aux sites concernés). Dans ce cas, le rôle du proxy comme filtre est proche du zéro pour vous mais important pour votre fournisseur d'accès. En effet, il peut grâce à son serveur proxy se générer une grande et belle base de données concernant ses utilisateurs (déterminer des profils d'utilisateur à des fins commerciales, quantifier les visites des sites et le temps passé dessus, etc.). Le meilleur moyen de juger votre protection est de se connecter au site du C.N.I.L (voir début de l'article).

1.7. Les anonymizers

Ces sites jouent le rôle de filtre total. En effet, vous utilisez leurs sites pour surfer de manière totalement anonyme. Il suffit de s'y rendre, puis d'entrer une requête (Essayez à nouveau le site du C.N.I.L par exemple). Les informations qui apparaissent sont celles du site d'anonymat et non plus les vôtres.

Il y a cependant deux inconvénients majeurs :

- ☞ le premier est qu'il faudra d'abord accéder au site d'anonymat puis entrer les URL de vos choix (les adresses des sites). Il y a donc une perte importante de temps.
- ☞ le second est le plus important. En effet, les sites que vous visitez via cet anonymizer n'ont plus accès à vos informations, mais l'anonymizer lui y a accès !!! Il peut donc en toute tranquillité se créer une base de données vous concernant en notant vos informations et les requêtes que vous avez entrées. De plus, et pour des motifs graves, un site peut remonter facilement à l'anonymizer, qui remontera alors jusqu'à vous...

Cet anonymat est donc très relatif...

Pour trouver un anonymizer, entrer la requête " anonymizer " dans un moteur de recherche.

1.8. Les fournisseurs d'accès gratuits, qui prônent l'anonymat...

Certains fournisseurs d'accès gratuits ne requièrent aucune information vous concernant (ni nom, ni adresse) et facturent seulement vos frais téléphoniques (via votre opérateur habituel). Là encore, vous êtes loin d'être anonyme. En effet, votre facture téléphone vous arrive chez vous. De plus, et pour quantifier vos consommations, ces fournisseurs utilisent vos adresses IP et MAC. Il est donc possible à ces fournisseurs de remonter facilement à vous. Enfin, la loi française oblige les fournisseurs d'accès à connaître l'identité de ses clients (via le téléphone par exemple).

1.9. Les logiciels qui intègrent des chevaux de Troie

Certains logiciels (utilitaires, jeux, ou mêmes des pilotes de périphériques) que vous installez sur votre ordinateur peuvent contenir des chevaux de troie. Par cheval de Troie (en référence à la mythologie grecque), on définit les programmes qui pénètrent à votre insu dans votre ordinateur. Ces programmes peuvent briser votre anonymat lorsque certaines conditions sont réunies et envoyer des informations confidentielles à des sites. Ainsi, certains exemples connus ont défrayé la chronique.

Le célèbre jeu Starcraft (Blizzard) possède un mode multijoueur sur Internet. Ainsi, vous pouvez jouer online sur les serveurs destinés à cet effet. Un utilisateur possédant un firewall (filtrage des données qui entrent et sortent lors d'une connexion) a remarqué que certaines informations circulaient pendant qu'il jouait. Il s'est avéré que la version commerciale du jeu contient un programme qui renseigne notamment le site sur le système d'exploitation utilisé, la version du navigateur, etc. Bien que destiné à éviter l'utilisation de copies illégales du jeu et partant donc d'une intention noble, cette opération est effectuée à l'insu de l'utilisateur et n'est mentionnée nulle part. Le site, dans ce cas là, ne procède pas à un stockage des informations mais pourrait très bien le faire.

Autre exemple célèbre : Les utilisateurs de processeurs Pentium 3 ont une option dans le bios de leur carte mère qui permet de dévoiler ou non un numéro d'identification (unique pour chaque processeur). Ce paramètre était activé par défaut sur certaines configurations et dévoilait donc ce numéro à la société Intel. Ce numéro permet là encore de remonter sinon à vous, au moins à l'endroit où a été envoyé le lot de processeurs.

Pour contrôler de manière efficace les données qui entrent et sortent de votre ordinateur pendant une connexion, utilisez un firewall. Ces pare-feu (traduction littérale) surveillent en permanence le flux de données de votre PC et vous signalent tout type de transfert suspect. Certains de ces programmes sont gratuits, comme Zonealarm, disponible sur "<http://www.zonelabs.com>".

1.10. Envoyer des mails anonymes

De nombreuses informations figurent sur un mail que vous envoyez avec votre messagerie habituelle. Celles-ci sont cachées par défaut mais peuvent être affichées très facilement. Sous Outlook par exemple, cliquez avec le bouton droit sur un message que vous avez reçu ou envoyé. Affichez les détails de ce message. Ceux-ci informent sur tous les destinataires du message, ainsi que leur adresse et les ordinateurs par lesquels ces messages ont transité. Admettons maintenant que vous envoyiez une demande de devis à une quinzaine d'entreprises. Celles-ci connaîtront facilement tous les autres destinataires du message (et leurs adresses e-mail).

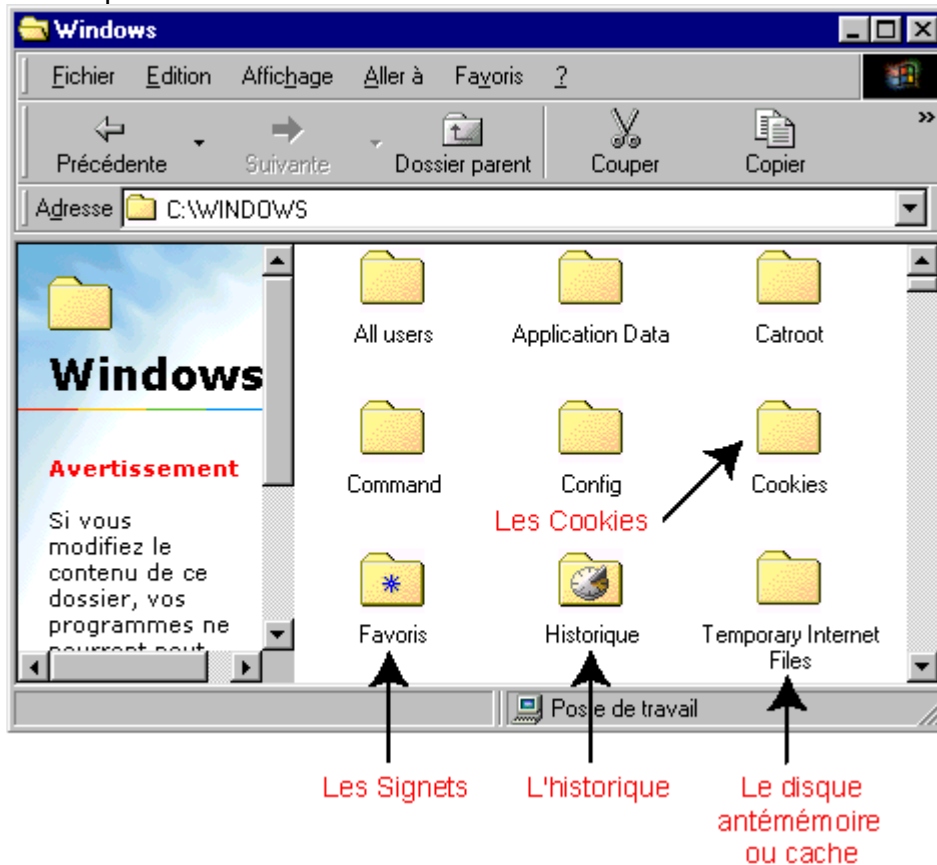
Pour contrer ce type de divulgation, vous pouvez avoir recours à des programmes ou des sites qui envoient les messages de manières anonymes. Ceux-ci masqueront alors toutes vos informations. En revanche et comme pour les anonymizers (voir paragraphe " les anonymizers "), le site ou le programme que vous utiliserez pour avoir cet anonymat possèdera quant à lui vos informations.

Tenter de nuire à quelqu'un en envoyant un message bourré de virus, d'insultes gratuites ou de menaces de mort, serait donc une erreur, puisque le destinataire aura accès au site qui a redirigé votre message. Celui-ci a bien évidemment notifié vos diverses adresses (IP, MAC) et pourra aisément remonter à vous dans les cas graves. Il est d'ailleurs heureux qu'il en soit ainsi, puisque cela protège les internautes des hackers patentés.

1.11. Les traces laissées sur votre disque dur

Votre disque contient de nombreuses informations créées lors de vos connexions. Il est possible alors, en accédant à votre ordinateur (directement ou par le biais d'un cheval de Troie) de reconstituer votre parcours sur Internet. Là encore, l'utilisation de ces informations est rare si vous

êtes un particulier connecté à votre domicile. En revanche, dans le cadre de votre entreprise, il est très facile de vous espionner.



1.12. Les Cookies

Ces petits programmes sont créés lors de visites sur certains sites. Si vous êtes sous Internet EXPLorer, ouvrez le dossier Windows, puis le dossier Cookies. Vous distinguez de nombreux fichiers texte (.txt). Ces fichiers ont souvent pour nom le vôtre (micheldurand@ " le nom du site ") et fournissent votre adresse IP, MAC, et bien d'autres informations cryptées (système d'eXPloitation, version du navigateur, etc.). Supprimer ces cookies ne sert à rien, puisqu'ils sont consignés dans le même répertoire dans le fichier Index.dat (Ce fichier est un fichier système et ne doit pas être supprimé !!). Il existe une manipulation qui est à réserver aux utilisateurs eXPérimentés :

- ☞ renommez le dossier cookies avec un autre nom (cookies1 par exemple).
- ☞ dans le même dossier Windows, créez un nouveau dossier "cookies". Malgré la création de ce nouveau dossier cookies, Wind menu exécuter, et entrez " regedit "). Ce programme modifie la base de registre. S'il est si difficile d' accès, c'est qu'il est dangereux à utiliser. Ne jouez jamais avec ce programme !
- ☞ rendez-vous grâce à l'eXPloreur regedit à la clé HKEYCURRENTUSER\Software\Microsoft\Windows\CurrentVersion\EXPLorer\User Shell Folders
- ☞ double-cliquez sur l'entrée "**cookies**", et modifiez le chemin en remplaçant " cookies1 " (l'ancien dossier contenant vos cookies) par " cookies " (le dossier vide que vous avez créé).
- ☞ après redémarrage, le système va créer le fichier système Index.dat dans votre nouveau dossier cookies qui sera vide.
- ☞ supprimez le dossier " cookies1 ". Vous effacez alors tous vos cookies antérieurs.
- ☞ répétez cette opération aussi souvent que vous le souhaitez. Celle-ci permet d'effacer votre passé sur Internet.

1.13. L'historique

Le dossier historique se trouve dans le dossier Windows . Il mémorise à différents pas de temps tous les sites que vous avez visités. EXPLorez-le et vous serez surpris. Il est utilisé pour rendre votre navigation plus confortable. En effet, lorsque vous entrez une adresse URL (un lien) dans votre navigateur, vous remarquez que celui-ci anticipe vos frappes (lorsque vous entrez ipt, un menu déroulant affiche iptsos.com par exemple). Ce système est bien entendu très pratique. Le

problème est que cet historique est conservé sur votre disque dur et est donc accessible à toute personne utilisant votre ordinateur (ou y ayant accès).

Avant toute manipulation, prenez en compte plusieurs choses : Supprimer l'historique ralentira votre navigation sur Internet. En effet, le dossier contient les pages entières. Si vous réglez l'historique sur zéro, vous devrez recharger en entier les pages des sites que vous visitez souvent, et ce, à chaque connexion. Si vous êtes connecté par modem téléphonique, essayez de trouver un compromis entre rapidité et anonymat. Si vous possédez une connexion à haut débit (câble, ADSL ou mieux), la perte de temps sera quasiment nulle (hormis en chargeant les pages très lourdes avec animations et images). Pour configurer ou supprimer votre historique, procédez comme suit :

- ☞ ouvrez votre navigateur
- ☞ placez-vous dans le menu "**Outils**" et sélectionnez "**Options Internet**"
- ☞ dans l'onglet général, vous avez trois types d'informations : la page à afficher au démarrage, le dossier Temporary Internet Files et enfin, l'historique. C'est cette dernière qui nous intéresse.
- ☞ vous pouvez entrer un nombre de jours pendant lequel ces pages sont conservées. Par défaut, cette option est réglée sur 20 jours. C'est à dire que vos 20 derniers jours de surf sont accessibles.
- ☞ modifiez ce paramètre à votre guise.
- ☞ vous pouvez également effacer l'historique (soit les 20 derniers jours), pour la remettre à zéro.



1.14. Le cache Temporary Internet Files

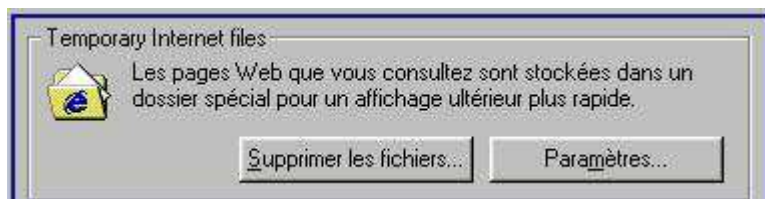
Ce sous-dossier se trouve dans le dossier Windows. Contrairement à l'historique où l'unité de mesure est le temps, les informations définies ici le sont par la taille. Ce dossier est un cache qui contient les dernières pages web visitées (des fichiers texte, des images, des animations). On l'appelle aussi disque antémémoire. Si vous êtes connecté par modem, vous avez certainement déjà remarqué que les sites ou vous allez souvent s'affichent très rapidement. C'est parce qu'elles sont stockées sur votre disque dur. Là encore, quelqu'un ayant accès à votre ordinateur (directement ou indirectement) peut disposer de ces informations comme bon lui semble. Ce dossier fonctionne comme un réservoir (dont la contenance est définie en Mo). Si la taille est de 50 Mo, l'ordinateur stockera toutes les pages web consultées jusqu'à que ce dossier soit plein. Ensuite, il remplacera les fichiers de manière intelligente (Ceux qui sont vieux et pas utilisés par les fichiers récemment consultés sur le Web). La taille sera toujours au maximum ensuite. Une telle taille permet de conserver très facilement plusieurs centaines de pages.

Pour modifier la taille de votre disque antémémoire, procédez comme suit :

- ☞ ouvrez votre navigateur
- ☞ dans le menu "**Outils**", sélectionnez "**Options Internet**".
- ☞ dans "**TemporaryInternetFiles**", choisissez "**Paramètres**"
- ☞ vous voyez apparaître la taille allouée à ce fichier. Modifiez là à votre guise.
- ☞ quelques paramètres sont là aussi à prendre en compte. Si vous surfez beaucoup, et n'utilisez que rarement les mêmes pages, vous pouvez entrer une taille faible (10 Mo). En effet, vous ne chargerez que rarement les mêmes pages. Si en revanche vous êtes un habitué de certains sites, il est préférable de stocker ceux-ci. Allouez alors une taille respectable (50 Mo).
- ☞ toujours dans le menu **Outils/OptionsInternet/Général/TemporaryInternetFiles**, vous pouvez supprimer les fichiers de ce répertoire. Si vous ne souhaitez pas

laisser trop de traces (dans votre entreprise par exemple), supprimez de temps à autre les fichiers de ce cache.

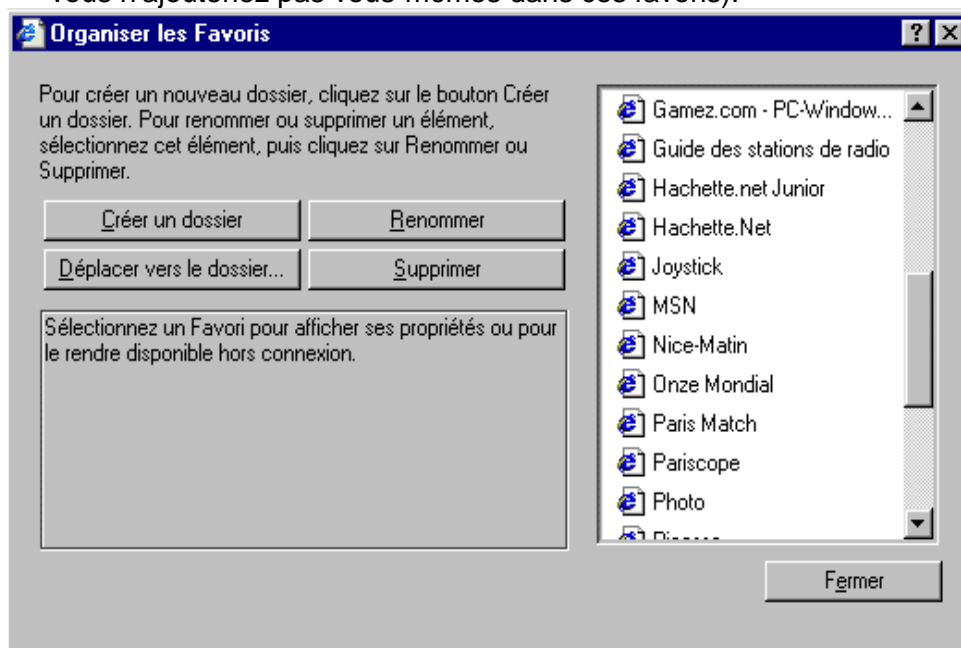
- enfin, et comme pour le paragraphe précédent, tout dépend de votre connexion. Si vous êtes connecté par modem téléphonique (lent), il est préférable de laisser ce dossier pour accélérer votre surf. La perte de temps est moindre si vous possédez une connexion à haut débit, puisque le chargement des pages est quasiment immédiat. Enfin, pour ceux qui possèdent des limitations en Download (câble et ADSL, tout sur l'ADSL ici), utilisez ce cache pour réduire le chargement des pages que vous fréquentez souvent.



1.15. Les signets ou favoris

Vous possédez sur votre navigateur une fonction qui permet de conserver les URL de vos sites préférés. Cette option est là aussi destinée à accroître le confort de l'internaute, en lui évitant de se remémorer les liens souvent longs et fastidieux. Elle permet aussi à toute personne ayant directement ou indirectement accès à votre ordinateur de consulter ces liens. Sous Internet Explorer, ces signets se nomment Favoris. Si vous voulez éviter de laisser des traces de ce type, supprimez ceux qui existent et évitez d'en ajouter de nouveaux.

- sélectionnez **Favoris** dans Internet Explorer.
- choisissez **Organiser** **Supprimez les signets que vous ne souhaitez pas voir apparaître**. Vérifiez également souvent ces favoris, car il est très facile d'en "attraper" à votre insu. Certains sites permettent le placement automatique dans les favoris simplement en cliquant sur un lien (une photo, etc.). Les sites sérieux vous le proposent pour raccourcir la manœuvre (les fonctions sur les pages web du type : " **Cliquez ici pour ajouter ce site à vos favoris** "). D'autres qui sont nettement moins recommandables ne vous avertissent pas (en général, les sites "osés" que vous n'ajouteriez pas vous-mêmes dans ces favoris).



1.16. Conclusion

Il est évident que l'anonymat total n'existe pas sur Internet. Tout au plus peut-on se rendre discret, et ce en exerçant une surveillance de tous les instants.

Pour toute information complémentaire sur le sujet :



- "<http://www.cnil.fr>": Il s'agit du site de la Commission Nationale de l'Informatique et des Libertés. Vous trouverez notamment de nombreuses informations juridiques et pratiques sur le sujet.

- "http://anonymat.org": Ce site est consacré à l'anonymat sur Internet. De nombreux dossiers exhaustifs et accessibles sont téléchargeables, ainsi qu'une foule de liens vers des anonymizers, des firewalls, ou des pages web pour tester votre système.

2 COMMENT VOTRE PC PEUT-IL ÊTRE PIRATÉ SUR INTERNET ?

Toujours le fait de personnes malveillantes, les risques inhérents à la sécurité informatique sont nuisibles à différents degrés.

Votre ordinateur est eXPosé à une multitude de risques de piratage via Internet qu'il est possible de regrouper selon deux catégories principales :

-  - La prise de contrôle à distance de votre ordinateur : bien souvent, un pirate prend le contrôle de votre PC (sans qu'aucun signe ne vous alerte) et l'utilise pour lancer une attaque beaucoup plus sévère contre un autre ordinateur connecté comme vous au réseau Internet. Son identité restera donc secrète puisque son méfait aura été lancé à partir de votre ordinateur.
-  - Le détournement d'informations vous concernant : dans ce cas, le pirate est capable de lire l'ensemble des fichiers enregistrés sur votre disque dur : courrier, documents personnels, liste d'adresses postales ou e-mails, etc. Outre la violation de votre vie privée, l'intrus peut récupérer des données beaucoup plus sensibles telles que des numéros de compte en banque, de cartes bancaires ou, dans le cas des entreprises, des informations confidentielles.

2.1. Le piratage nous concerne tous

Depuis l'avènement de l'ère Internet à la fin de années 90, le nombre d'ordinateurs connectés à Internet ne cesse d'augmenter. Internet étant un réseau mondial, libre de tout contrôle, il présente de nombreux avantages : échange gratuit d'information en temps réel, communication instantanée par e-mails, messagers ou par visioconférence, etc.





Malgré ses nombreux avantages, le plus grand des réseaux présente néanmoins des risques avérés en matière de sécurité informatique dont vous avez déjà probablement entendu parler. Ainsi, certaines personnes malveillantes n'hésitent pas à utiliser certaines failles logicielles et matérielles pour s'approprier des données personnelles ou confidentielles à votre insu. C'est également en utilisant cette voie que les pirates du Net diffusent virus et autres logiciels informatiques nuisibles quelques fois destinés à prendre le contrôle de votre ordinateur. Un ordinateur connecté à Internet sans aucune précautions s'eXPose donc à l'attaque de ses données.

2.2. Quel est le risque d'une connexion ADSL ou d'un modem câble ?

Si vous disposez d'une connexion haut débit ADSL ou via le câble active en permanence, les risques sont plus grands car votre ordinateur n'est pas une cible mouvante. Ainsi, lorsque vous utilisez une connexion d'accès à distance, l'adresse réseau de votre ordinateur est différente à chaque fois ; avec une connexion ADSL ou câble, en revanche, l'adresse réseau est inchangée pendant de longues périodes de temps (24 h. maximum). Si cette connexion permanente est un avantage, l'adresse de votre ordinateur est encore plus eXPosée aux pirates. Il existe également un risque lié au partage de la connexion : les personnes qui, dans votre entourage, partagent le même service de câble, peuvent potentiellement accéder à votre ordinateur si vous ne disposez d'aucune protection par pare-feu (ou **firewall**).

2.3. Que peut faire un pirate qui s'est introduit dans mon ordinateur ?

Non seulement les pirates cherchent à accéder à des informations privées, telles que des enregistrements financiers ou des fichiers de mots de passe, mais ils se servent aussi des ordinateurs aux fins suivantes :

-  - Lancer des attaques de déni de service (DoS - Denial of Service) contre un site Web en vue.
-  - Après en avoir pris le contrôle, le pirate peut contraindre votre ordinateur ainsi que des centaines, voire des milliers d'autres "zombies" à agir simultanément, ce qui surcharge un site populaire et provoque son indisponibilité.
-  - Distribuer des logiciels de façon illicite.
-  - Après s'être approprié l'espace sur votre disque dur, ils permettent à d'autres d'accéder à votre ordinateur en tant que site "warez" et de télécharger des divertissements ou des applications piratées.

3 LE PIRATAGE PAR L'ATTAQUE IP

De nombreux particuliers possédant un ordinateur personnel estiment ne pas avoir besoin de protéger les données contenues sur leurs disques durs. Il est en effet peu probable qu'un pirate de l'Internet s'intéresse à la photo du chat ou des enfants. En effet, le vrai pirate s'attaque en général aux serveurs afin d'en récupérer les données qu'il pourra revendre par la suite. Mais il est une catégorie de pirates amateurs qui se feront le plaisir de s'entraîner sur un ordinateur personnel avant de passer à l'échelon supérieur. C'est de cette catégorie qu'il est nécessaire de se protéger.

Vous êtes un particulier et vous doutez encore ? Suivez attentivement notre exemple :

Etape 1 : vous pouvez trouver très facilement (moins de 3 minutes) sur Internet un logiciel permettant de récupérer les adresses IP de chaque ordinateur connecté au réseau Internet. L'IP est une sorte d'immatriculation ou d'adresse de votre ordinateur à un instant t sur le réseau internet. Un récupérateur d'adresses IP appelé scanner inventorie donc toutes les adresses IP utilisées par les ordinateurs connectés à Internet au même moment. Le nombre d'IP étant de plus plusieurs milliards, la recherche d'IP se fait par tranche d'adresse : ici de 212.194.132.1 à 212.194.132.254.

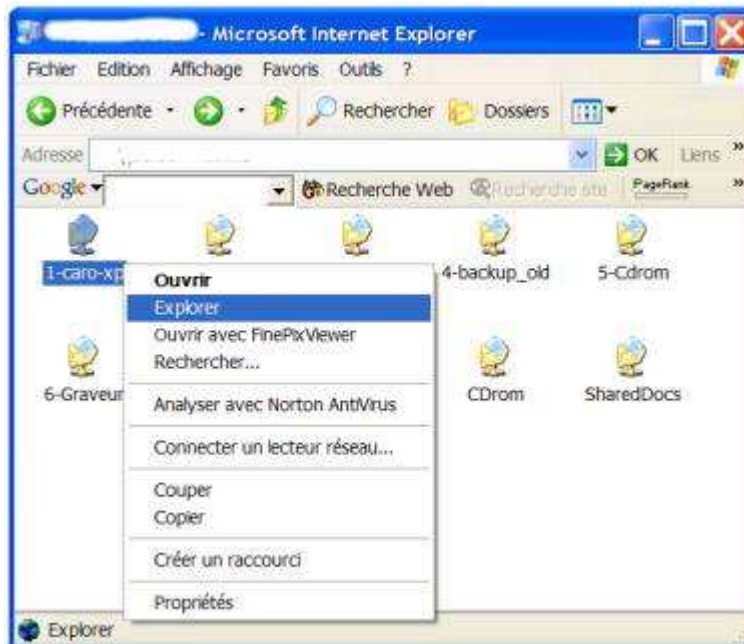
ATTENTION : l'utilisation d'un scanner de port ou d'IP est considéré en soi comme un acte de piratage même si vous ne pénétrez pas au sein des ordinateurs dont l'IP est listée. Notre exemple est à but pédagogique et ne doit pas être en aucun cas considéré comme une incitation au piratage.



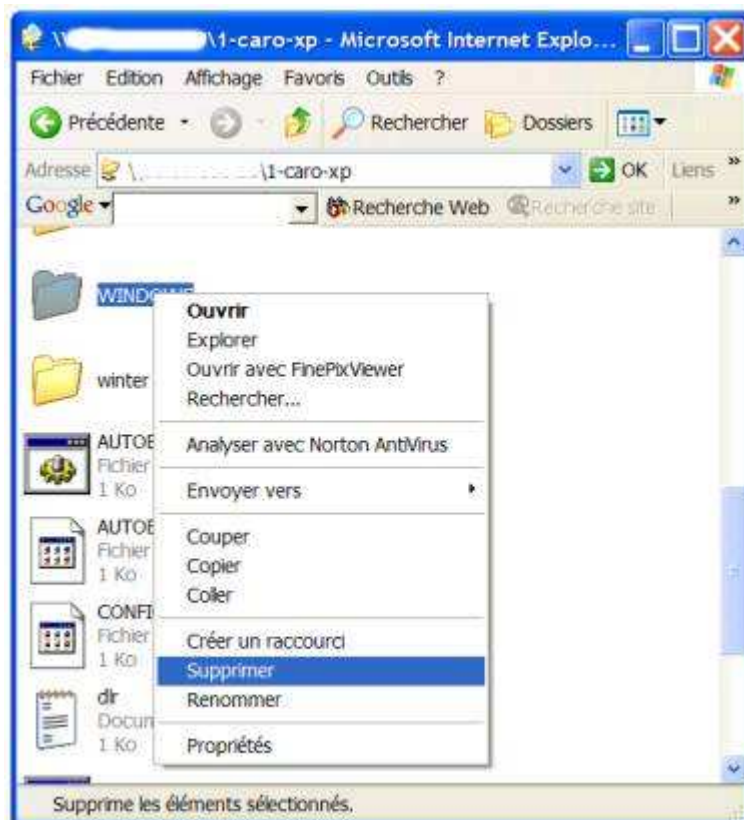
Etape 2 : Certains de ces ordinateurs connectés peuvent contenir des répertoires ou des disques durs partagés. Il s'agit d'éléments communs accessibles par plusieurs utilisateurs au sein d'un réseau. Le logiciel que nous utilisons permet également de savoir si un ordinateur contient ce type de répertoire ou ce type de disque.

Il suffit alors de taper l'adresse IP de l'ordinateur en question dans un navigateur internet (Internet EXPlorer par exemple) pour pouvoir afficher ses ressources partagées et y entrer comme si vous eXPloriez un des répertoires situés sur votre ordinateur.

Ici le contenu d'un ordinateur relié à Internet. Son utilisatrice qui s'appelle probablement Caroline possède plusieurs disques durs partagés dont le disque dur principal "Caro-XP" (Nous supposons qu'il s'agit du disque contenant le système d'eXPloitation Windows XP). La navigation entre les répertoires et les données sur un ordinateur distant est identique à celle que vous utilisez couramment sur le votre.



Etape 3 : Le disque dur Caro-XP contient le répertoire Windows ainsi que les fichiers utilisés lors du démarrage de l'ordinateur. Il est alors possible d'effectuer sur ces éléments toute sorte d'opérations ; modification du nom du dossier ou suppression de ce répertoire par exemple. L'utilisatrice de cet ordinateur ne pourrait de ce fait plus démarrer son ordinateur. Nous n'irons pas bien sûr jusque là, le but de notre exemple étant de vous montrer que les données de vos disques durs, même les plus importantes sont vulnérables dès lors que vous surfez sur Internet sans aucune protection. Notez qu'un mauvais pirate supprime vos données... un pirate qui se respecte vous prévient en créant ou en renommant un fichier, guère plus.



4 COMMENT SE PROTÉGER DES ATTAQUES PAR INTERNET

4.1. Protection des partages de fichiers

Windows XP utilise un modèle d'accès réseau appelé "partage de fichiers simple" où toutes les tentatives de connexion à l'ordinateur à distance sont contraintes d'utiliser le compte Invité.

Dans le modèle de partage de fichiers simple, il est possible de créer des partages de fichiers pour que l'accès à partir du réseau soit limité à la lecture ou étendu à la lecture, la création, la modification et la suppression de fichiers. Ce modèle est destiné à une utilisation en réseau domestique et derrière un pare-feu tel que celui fourni par Windows XP. Si vous êtes connecté à Internet sans être protégé par un pare-feu, vous devez garder à l'esprit que tous les partages de fichiers que vous créez risquent d'être accessibles à n'importe quel utilisateur d'Internet.

Pour contrôler les partages de fichiers, ouvrez votre **EXPlorateur Windows**.

Faites un clic avec le bouton droit de la souris sur le dossier de votre choix, ce peut être le disque dur lui-même, puis cliquez sur l'onglet **Partage et sécurité**. Dans la fenêtre **Propriétés**, activez les options de partage de votre choix. Cliquez sur le bouton **Appliquer** afin de prendre en compte les modifications.

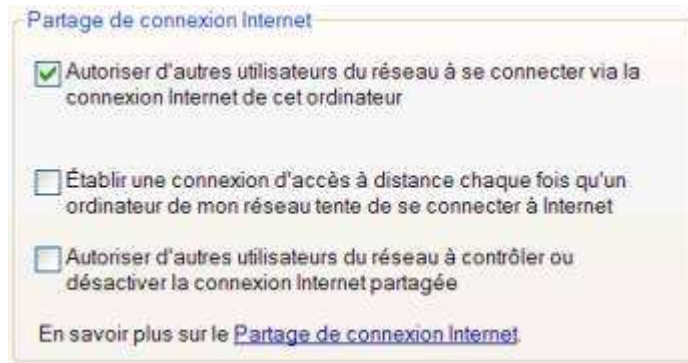
Il est néanmoins fort déconseillé d'autoriser les utilisateurs distants à modifier vos données. Ces derniers peuvent être des collègues de travail dont l'ordinateur est en réseau avec le votre ou des internautes cherchant à vous pirater.



4.2. Utilisez le partage de connexion pour les connexions Internet partagées

Windows XP vous donne la possibilité de partager une même connexion Internet entre plusieurs ordinateurs d'un réseau domestique ou de petite entreprise grâce à la fonctionnalité de partage de connexion Internet. L'un des ordinateurs, appelé hôte, se connecte directement à Internet et partage sa connexion avec les autres ordinateurs du réseau. Les ordinateurs clients dépendent de l'hôte pour obtenir l'accès à Internet. Ce fonctionnement améliore la sécurité dans la mesure où seul l'hôte est visible sur Internet :

Pour activer le partage de connexion internet, cliquez avec le bouton droit sur une connexion Internet dans **Connexions réseau**, cliquez sur **Propriétés**, cliquez sur l'onglet **Avancé**, puis cochez la première case.



4.3. Utilisation d'un pare-feu ou Firewall

Des millions d'ordinateurs sont aujourd'hui connectés au réseau Internet, du simple particulier à la grosse entreprise. Or être connecté signifie ouvrir son ordinateur au monde extérieur. La fonction de base d'un pare feu (ou firewall) est simple : il bloque tous les échanges entre un ordinateur et l'extérieur (que cela soit un réseau local ou Internet). C'est l'utilisateur qui, par la suite, détermine les autorisations d'accès aux programmes communiquant avec l'extérieur.

4.3.1. Principe du Firewall ou pare-feu




A chacune de vos connexions au réseau Internet, une adresse IP (x.x.x.x) est attribuée à votre ordinateur par le fournisseur d'accès auquel vous avez souscrit un contrat de connexion. Cette adresse permet d'identifier l'ordinateur sur le réseau. Elle est unique et dynamique, c'est à dire qu'elle change à chaque reconnexion (sauf cas particuliers : certains ordinateurs d'entreprise ont une adresse IP fixe).

Cette adresse est utilisée par les pirates pour pénétrer, ou tenter de le faire sur un ordinateur. Dès que l'adresse IP d'un ordinateur est trouvée, il suffit de scanner les ports pour voir quels sont ceux qui sont ouverts.

Un ordinateur PC sous Windows dispose de 65000 ports soit 65000 portes d'entrée différentes pour y accéder. Si tous ces ports ne sont pas accessibles, certains peuvent être utilisés pour pénétrer à l'intérieur d'un ordinateur. Il faudra toutefois qu'il y ait un programme présent sur l'ordinateur, permettant d'en prendre le contrôle de l'extérieur.







Ici intervient le concept de Cheval de Troie (Trojan Horse). Un Cheval de Troie est un programme installé sur l'ordinateur, souvent à l'insu de son utilisateur. Ce programme pourra être "activé" de l'extérieur, en utilisant un des ports de l'ordinateur. Une fois activé, il permettra à l'utilisateur de l'ordinateur distant, de prendre tout ou partie du contrôle de l'ordinateur local.

Pour éviter cela, il faut :

-  vérifiez la présence ou non d'un Cheval de Troie sur votre ordinateur avec un antivirus, vous pouvez par exemple contrôler cela en ligne.
-  utiliser un firewall pour bloquer les ports et ainsi empêcher l'intrusion ou la prise de contrôle à distance de votre PC.
-  Il est également vivement recommandé de mettre à jour fréquemment son Windows en utilisant Windows Update. Ceci corrigera les éventuelles failles découvertes dans le système d'exploitation.

Le firewall bloque les ports disponibles, et ne laisse ouverts que ceux qui sont nécessaires à l'utilisateur.

4.3.2. Les ports utilisés fréquemment par votre ordinateur

-  Ports 20 et 21 : FTP téléchargement de fichiers
-  Port 25 : SMTP envoi de courrier
-  Port 80 : HTTP navigateur Internet
-  Port 110 : POP3 réception de courrier
-  Port 119 : NNTP forums de discussion
-  Port 1014 : Utilisé pour le partage de fichiers sous le logiciel Kazaa

5 CHOISIR UN FIREWALL

5.1. A quoi sert un firewall ?

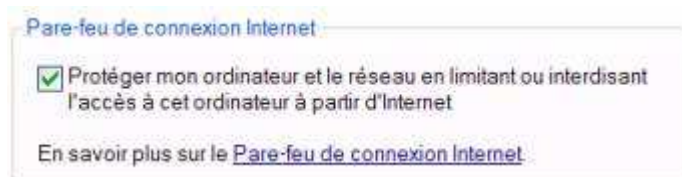
Avant de connecter votre ordinateur à Internet, vous devez installer un pare-feu. Un pare-feu est un matériel ou un logiciel qui empêche les pirates, ainsi que de nombreux types de virus et de vers, d'accéder à votre ordinateur. Si vous disposez du système d'exploitation Microsoft Windows® XP, vous pouvez utiliser son pare-feu de connexion Internet intégré. Un pare-feu constitue la première ligne de défense la plus importante pour la sécurité de votre ordinateur. Vous devez également utiliser Windows Update et un logiciel antivirus pour protéger votre PC.

Le pare-feu de connexion Internet bloque certains types de communications réseau potentiellement dangereuses. Cependant, il bloque également certaines tâches de communication réseau utiles (par exemple, le partage de fichiers ou d'imprimantes sur un réseau, le transfert de fichiers dans des applications telles que la messagerie instantanée, ou l'hébergement de jeux multijoueurs). Nous vous conseillons vivement d'utiliser un pare-feu car il vous permet de garantir la sécurité de votre ordinateur.

5.2. Le firewall de Windows XP

Conçu pour les réseaux domestiques ou ceux des petites entreprises, le Pare-feu de connexion Internet (ICF, Internet Connection Firewall) protège les ordinateurs connectés directement à Internet et les ordinateurs ou périphériques connectés à l'ordinateur hôte dans le cadre d'un partage de connexion internet. Le pare-feu ICF de Windows XP utilise un filtrage de paquets actif, c'est-à-dire que les ports du pare-feu sont ouverts dynamiquement et seulement pendant la durée nécessaire pour vous permettre d'accéder aux services qui vous intéressent.

Pour activer le pare feu XP, cliquez sur le bouton **Démarrer** puis placez votre pointeur (sans cliquer) sur la connexion Internet que vous utilisez couramment. Cliquez dessus avec le bouton droit de la souris et sélectionnez la ligne **Propriétés**. Cliquez sur l'onglet **Avancé**, puis activez la case située dans la zone **Pare-feu de connexion Internet**.



Si votre PC est en réseau et utilise une connexion Internet d'un autre poste, appliquez cette même procédure pour la Connexion au réseau local. Cliquez sur le bouton **Démarrer** puis sélectionnez **Panneau de Configuration**. Double cliquez sur l'icône **Connexions Réseau**. Cliquez avec le bouton droit de la souris sur l'icône **Connexion au réseau local** et sélectionnez **Propriétés**. Cliquez sur l'onglet **Avancé**, puis activez la case située dans la zone **Pare-feu de connexion Internet**.

Comment faire sous une autre version de Windows ?



Les versions de Windows antérieures à Windows XP n'incluaient pas de pare-feu intégré. Si votre ordinateur utilise une version antérieure de Windows, telle que Windows 2000, Windows Millennium ou Windows 98, vous devez acquérir un pare-feu puis l'installer. Vous pouvez utiliser un pare-feu matériel ou logiciel. Vous trouverez ci-dessous des informations complémentaires sur les différentes options qui s'offrent à vous en matière de pare-feu.




5.2.1. - pare-feu matériels

Les fabricants de points d'accès sans fil destinés aux réseaux privés proposent souvent des appareils qui intègrent un pare-feu matériel et un routeur pour accès à haut débit. La mise en œuvre d'un pare-feu matériel dans votre réseau est aussi simple que brancher un répondeur sur votre ligne téléphonique. Il vous suffit de débrancher le câble Ethernet qui relie votre PC à votre modem ADSL ou à votre modem câble, et d'insérer le pare-feu entre les deux.

5.2.2. - pare-feu logiciels

Vous pouvez acquérir des pare-feu logiciels auprès de différents fournisseurs, notamment :

-  Internet Security Systems : BlackIce PC Protection
-  Kerio : Kerio Personal Firewall

-  McAfee : Personal Firewall
-  Symantec : Norton Personal Firewall
-  Zone Labs : Firewall ZoneAlarm Pro

5.2.3. Zone Alarm : le firewall gratuit

Des millions d'ordinateurs sont aujourd'hui connectés au réseau Internet, du simple particulier à la grosse entreprise. Or être connecté signifie ouvrir son ordinateur au monde extérieur. La fonction de base d'un firewall est simple : il bloque tous les échanges entre un ordinateur et l'extérieur (que cela soit un réseau local ou Internet). C'est à l'utilisateur de déterminer les autorisations d'accès aux programmes qui communiquent avec l'extérieur.

Il existe de très nombreux logiciels de firewall, aux fonctions plus ou moins complexes en fonction du niveau de sécurité que vous souhaitez adopter. Développé par ZoneLabs, Zone Alarm est à la fois simple d'accès et efficace. Sa popularité est due à sa gratuité dans sa version de base, mais néanmoins amplement suffisante pour un usage domestique.

6 LES SPYWARES

6.1. Définition

Le spyware est aussi appelé espioniciel. Son rôle consiste à rassembler un maximum d'informations sur vous, et/ou vos habitudes sur Internet, parfois même en dehors, mais toujours en relation avec votre utilisation d'un PC, soit à domicile, soit durant votre travail. Une base de données va servir à rassembler toutes ces informations, en vue de vous sensibiliser sur tels ou tels produits, susceptibles de vous intéresser. Par la suite, vous allez recevoir des publicités vantant ces produits. Là, nous sommes en présence de sociétés cherchant à vendre, donc purement marketing. Certaines de ces sociétés en profitent pour revendre ces informations à leurs clients. Bref, si vous pensiez échapper à la publicité... C'est raté. La méthode est simple.

6.2. Comment les spywares arrivent-ils sur votre PC ?

Vous avez besoin d'un logiciel; vous allez le chercher si possible gratuitement. L'éditeur va vous le proposer en vous demandant d'accepter un contrat préalable, et accompagné d'un certificat de confiance. Très souvent, la collecte des informations vous concernant y est clairement lisible.

En acceptant, vous vous engagez à ne pas supprimer le fichier chargé de recueillir et retransmettre ces informations. Si vous le faites tout de même, il est fort possible que le logiciel que vous convoitez, ne fonctionne plus. Vous serez amené à le désinstaller, mais l'espion restera probablement en place. Ceci est la version commerciale du spyware.

6.3. Des spywares installés à votre insu !

Malheureusement, il existe aussi une version plus odieuse du spyware. Celle-ci se fait complètement à votre insu. Vous ne saurez être victime d'un de ces spyware, qu'au moment où vous constaterez ses effets. Vous aviez une belle page de démarrage, or vous vous retrouvez ailleurs. Dès que vous lancez votre navigateur Internet, vous n'êtes pas sur votre portail mais bel et bien sur un site que vous n'avez jamais ou seulement une fois fréquenté. Vous recherchez des informations ou pages Internet avec Google ou autre moteur de recherches, et vous voilà face à un moteur de recherches que vous ne connaissez pas. Autre effet possible, vous avez la fameuse toolbar sur votre eXPlorateur, vous vous retrouvez affublé d'une seconde barre. Vous êtes victime d'un hijacker.

Vous allez sur Internet grâce à un modem ADSL ou câble, et lorsque vous lancez votre navigateur, vous avez une demande de connexion ou lancement RNIS; dans ce cas, vous avez affaire à un dialer. Et le plus souvent, il s'agit de sites commerciaux à des tarifs élevés (en général sites à contenu érotique), que vous retrouverez sur votre facture de téléphone.

6.4. Exemples de Spywares

Les Spywares publicitaires : ils sont intégrés dans des programmes bien souvent gratuits qui permettent de rentabiliser la création de ces logiciels. Les plus connus sont : Aureate/Radiate, Conducent/Timesink, Web 3000, Cydoor, Gator (il change de nom pour Claria), WebHancer, EverAd, Onflow, Comet Cursors, New.net, SaveNow, TopText, Alexa etc ! Les logiciels qui intègrent ce type de spywares : Babylon Translator, Cute FTP, EuroConverter 2, Free MP3, Gator,

Zip eXPress 2000, ICQ, RealJukebox, Imesh, Kazaa et des milliers d'autres ! Les spywares publicitaires sont en général ceux qui bugs le plus et surtout les plus critiquables sur l'espionnage à grande échelle des internautes. Ce sont ceux qui polluent le plus et les plus difficiles à déjouer et à supprimer ! en effet la suppression du programme en question par exemple babylon n'implique pas forcément la suppression du spyware ! en résumé il reste bien souvent après la suppression du logiciel.

Les Spywares à but commercial : Les premiers du genre ont été bien sûr Microsoft, Netscape et Real Player. D'ailleurs ils continuent d'agir promptement ! Mais en général même si ce sont les plus vicieux dans leur méthode ils sont en général pas forcément les plus dangereux.

6.5. Dangereux ou pas ?

Pour la protection de votre vie privée, oui . Dans la plupart des cas les sociétés éditrices de ce type de logiciel gardent bien caché les réelles informations sur ce sujet délicats. On ne peut par ailleurs que se poser la question puisque dans la plupart des cas les spywares sont intégrés à l'insu des utilisateurs.

Il existe de gros problèmes également au niveau de la stabilité des ordinateurs infestés, en effet dans la plupart des cas cela engendrent des plantages, de très grosses lenteurs de votre système et des problèmes de connexion à Internet voire des failles. De plus ils le font souvent sans que vous en rendiez compte ou essayent de mieux vous entourloupier en vous proposant de vous rendre service.

6.6. Détecter et supprimer les spywares

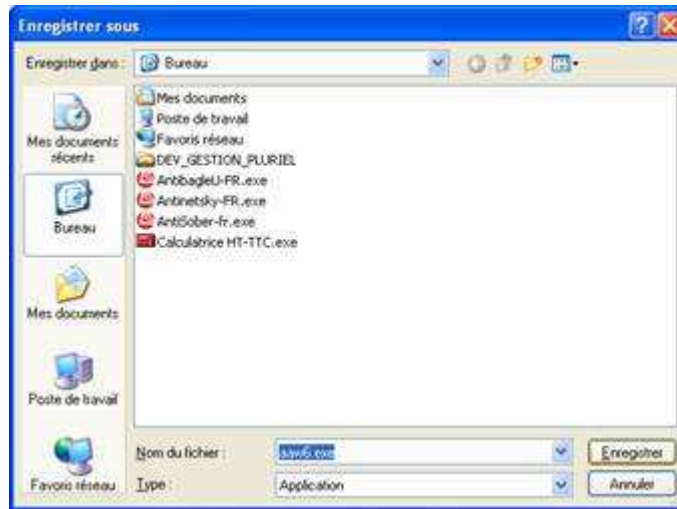
Ils existe deux très bons outils pour détecter et supprimer les spywares de votre ordinateur qui sont les utilitaires Ad Aware et SpyBot "Search and Destroy". Il en existe de très nombreux autres, un peu plus complexes en terme de prise en main.

7 INSTALLATION DE L'ANTI SPYWARE AD AWARE

Etape 1 : Télécharger le logiciel gratuit Ad Aware en vous rendant sur le site **Lavasoft**, l'éditeur d'Ad Aware d'où il est possible de le télécharger. Lors de l'ouverture de la fenêtre de téléchargement, cliquez sur le bouton **Enregistrer** avec le bouton gauche de la souris.



Etape 2 : Nous vous conseillons de télécharger le programme d'installation d'Ad aware sur votre bureau. Ainsi vous pourrez le supprimer très rapidement dès que le programme sera définitivement installé. Le téléchargement prend entre 20 secondes et 2 minutes en fonction de la vitesse de votre connexion.



Etape 3 : Double cliquer sur le programme d'installation d'Ad Aware que vous venez de télécharger et suivez les instructions à l'écran. Il s'agit en fait de cliquer sur le bouton **Next** à chacun des écrans du programme d'installation. Le programme Ad Aware est en effet en langue anglaise par défaut, mais cela n'est pas un handicap car son utilisation est enfantine.

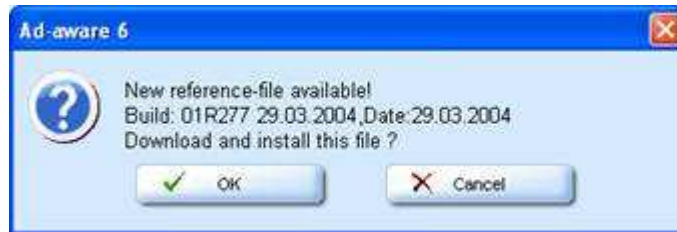


Lancer une analyse anti spyware avec Ad Aware

Etape 1 : Lancez le programme Ad Aware en cliquant sur le bouton **Démarrer**, Placez votre pointeur sur **Tous les programmes**, puis sur **Lavasoft – Ad aware** et cliquez sur la ligne **Ad-Aware**.



Etape 2 : Il se crée sur internet plusieurs spywares par jour (un peu comme pour les virus). Aussi nous allons commencer par effectuer une mise à jour d'Ad Aware, ce qui permettra à ce dernier de reconnaître les spywares découverts récemment. Pour cela cliquez sur le lien **Check for updates now**. Cliquez ensuite sur le bouton **Connect**. Cette procédure permet au programme de contrôler sur le serveur de son éditeur la présence ou non de mises à jour. En cas de mise à jour présente, veuillez confirmer l'installation de cette dernière en cliquant sur le bouton **OK** et patientez quelques secondes. Cliquez sur le bouton **Finish** pour terminer la procédure de mise à jour.



Etape 3 : Tout est maintenant prêt pour une analyse des données de votre ordinateur. Cliquez sur le bouton **Start** et validez les options d'analyse par défaut en cliquant sur le bouton **Next**.



Etape 4 : L'analyse prend de 3 à 10 minutes en fonction de la densité des fichiers de votre ordinateur. Le nombre de fichiers considérés comme parasites est affiché en temps réel.



Etape 5 : L'analyse terminée, cliquez sur le bouton **Next** afin de prendre connaissance des fichiers parasites détectés par Ad Aware. A noter qu'Ad Aware référence les programmes publicitaires, les programmes espions et les cookies (Tracking Cookie). Ces derniers fichiers sont inoffensifs et il n'est pas forcément nécessaire de les supprimer. Sélectionnez alors les fichiers et programmes parasites trouvés que vous souhaitez supprimer en cochant la case associée. Si vous ne savez pas quoi choisir, sélectionnez cochez toutes les cases et cliquez sur le bouton **Next**.



Etape 6 : Confirmez la suppression des fichiers et programmes cochés en cliquant sur le bouton **OK**.



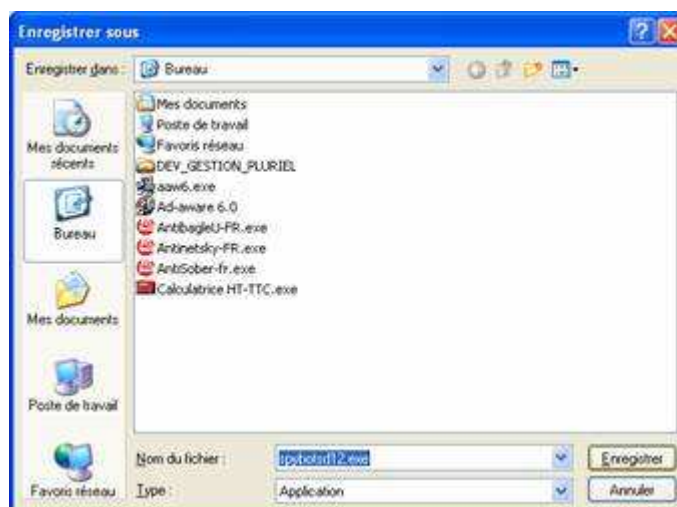
8 INSTALLATION DE L'ANTI SPYWARE SPYBOT "SEARCH AND DESTROY"

Spybot est un utilitaire gratuit permettant de débusquer les programmes parasites, les logiciels espions, mais aussi les failles de sécurité de votre ordinateur. Il est considéré à juste titre comme un logiciel de protection de la vie privée.

Etape 1 : Télécharger le logiciel gratuit SpyBot en cliquant sur ce lien ou rendez-vous sur le site de l'éditeur, d'où il est également possible de le télécharger. Lors de l'ouverture de la fenêtre de téléchargement, cliquez sur le bouton **Enregistrer** avec le bouton gauche de la souris.



Etape 2 : Nous vous conseillons de télécharger le programme d'installation Spybot sur votre bureau. Ainsi vous pourrez le supprimer très rapidement dès que le programme sera définitivement installé. Le téléchargement prend entre 1 minute et 5 minutes en fonction de la vitesse de votre connexion.



Etape 3 : Double cliquez sur le programme d'installation Spybot que vous venez de télécharger et suivez les instructions à l'écran. Cliquez sur les boutons **Next** puis sur **Install** et **Finish** en fin de procédure.



Lancer une analyse anti spyware avec SpyBot

Etape 1 : Lancez le programme SpyBot en cliquant sur le bouton **Démarrer**, Placez votre pointeur sur **Tous les programmes**, puis sur **Spybot – Search And Destroy** et cliquez sur la ligne **SpyBot – S&D (Easy Mode)**.



Etape 2 : Il se crée sur internet plusieurs spywares par jour (un peu comme pour les virus). Aussi nous allons commencer par effectuer une mise à jour de SpyBot, ce qui permettra à ce dernier de reconnaître les spywares et logiciels espions découverts récemment. Pour cela cliquez sur le lien **Recherche de mise à jour**. Puis cochez les mises à jours proposées puis cliquez sur le bouton **Télécharger les mises à jour**. Cette opération peut durer plusieurs minutes en fonction de la vitesse de votre connexion à Internet.



Etape 3 : Une fois les différentes mises à jour téléchargées, lancez l'analyse en cliquant sur le bouton **Vérifier tout**. Les logiciels parasites, espions et les failles de sécurité s'affichent dans la fenêtre centrale de Spybot au fur et à mesure qu'ils sont détectés. Une fois l'analyse complètement

terminée, cliquez sur le bouton **Corriger les problèmes** ce qui aura pour effet soit de supprimer les logiciels parasites ou espions et de colmater les failles de sécurité de votre système. Confirmer ce choix en cliquant sur le bouton **OK**. Vous pouvez maintenant fermer le programme SpyBot.



Etape 4 : Il est conseillé de redémarrer votre ordinateur après l'analyse Spybot. Renouvelez cette dernière une fois par mois afin d'assainir votre ordinateur.

9 LES PEER TO PEER (P2P)

Kazaa, mais aussi **Gnutella**, **Limewire**, **eDonkey**, **Grokster**, **Imesh**, sont des logiciels **P2P**, autrement dit "**Peer to Peer**". Lorsque vous les installez, vous devenez membre d'un réseau d'échange de fichiers via Internet extrêmement puissant. Vous pourrez y télécharger tout ce que les membres ont placé sur leur ordinateur dans un répertoire dédié, mais les mêmes membres pourront également voir ce que vous avez mis dans le répertoire équivalent, et le télécharger à leur tour. Il s'agit donc d'un échange d'ordinateur à ordinateur.



L'utilisation la plus courante sur les réseaux Peer to Peer est l'échange de fichiers MP3 (système de compression du son, qui permet de réduire considérablement le poids des fichiers des CD audio). Les fichiers MP3 sont en fait des fichiers musicaux contenant une chanson, voire tout l'album d'un auteur. Mais on trouve également au sein de ces réseaux d'autres documents comme des images, des films (appelés divX), des jeux vidéo ou des logiciels piratés.

9.1. Le Principe d'utilisation

L'accès à un réseau Peer to Peer débute presque toujours par l'installation sur son ordinateur d'un logiciel de connexion. Ce logiciel est alors utilisé pour se connecter au réseau P2P en utilisant votre connexion à Internet.

Dés lors, il vous suffit d'indiquer le titre d'une chanson ou d'un document dans l'interface de recherche du logiciel installé et il vous est affiché une liste des ordinateurs connectés au même réseau qui contiennent le fichier pouvant correspondre à votre recherche. Il vous suffit alors de cliquer sur l'une ou l'autre de ces réponses pour télécharger le fichier en question sur votre ordinateur. Une fois ce fichier téléchargé sur votre disque dur, il est à nouveau mis à la disposition des autres utilisateurs du réseau. C'est le principe même de l'échange de données.

9.2. Ce que dit la loi

Le Peer to Peer en soit est légal, c'est l'utilisation qui en est fait qui ne l'est pas !

La loi est très claire sur ce point : il est interdit d'échanger des œuvres pour lesquelles vous n'avait pas payer de droit d'auteurs. Télécharger un fichier et le mettre à la disposition des autres internautes fait de vous un pirate.

Il en va de même si vous disposez à votre domicile d'un CD original et que vous partagez sur Internet les différents titres de ce disque. La copie est certes légale dans un but de sauvegarde, mais rien ne vous autorise à offrir ces copies à d'autres internautes, même si cela n'entraîne aucun échange d'argent.

Outre cela, un tel comportement met en péril la situation des auteurs des œuvres téléchargées. Ceux-ci étant payés en fonction du nombre de disques vendus, il est évident que si vous parvenez à télécharger ces disques gratuitement, ils ne toucheront pas de droits. Aimerez-vous travailler sans être payé ?

Le danger n'est pas seulement pour les auteurs piratés. Il est également pour ceux qui téléchargent. Que ceux qui se croient anonymes sur Internet s'en rendent compte rapidement : tout internaute peut être pisté sur Internet par différents moyens. D'autre part, les fournisseurs d'accès à Internet (FAI) peuvent être contraints par la Justice à révéler les identités des personnes qui utilisent les réseaux Peer to Peer dans un cadre non légal.

9.3. Les autres risques sur l'utilisation des réseaux Peer to Peer

Mais il y a un autre risque, plus insidieux. Kazaa, comme de nombreux autres logiciels gratuits, Kazaa contient des "espioniciels", logiciels destinés à observer vos habitudes de consommation sur Internet afin de mieux vous démarcher par la suite. Ces logiciels communiquent aux sociétés liées à Kazaa un très grand nombre de données telles que adresses email, sites visités, durée de connexion, et dans certains cas révélés vos informations bancaires. Certains espioniciels peuvent aussi prendre le contrôle de l'ordinateur et utiliser sa puissance de calcul. Voilà pourquoi les ordinateurs sur lesquels sont utilisés un ou plusieurs logiciels de connexion Peer to Peer peuvent être très lents.

Ce problème ne touche pas seulement Kazaa. Plus de 1000 logiciels gratuits ont ainsi été dénoncés comme camouflant des espioniciels, seule manière trouvée par les développeurs pour amortir le coût de développement de leur produit. Des logiciels gratuits ont heureusement été développés pour lutter contre ces mouchards virtuels. Mais la meilleure protection, dans tous les cas, est de ne pas télécharger Kazaa, de le fuir comme la peste, d'interdire totalement son utilisation sur votre ordinateur et de vous tourner vers des alternatives comme le téléchargement légal d'œuvres musicales à bas prix (exemple : un titre = 0.70 € sur certains sites spécialisés).


10 RETIRER LE MOUCHARD DE WINDOWS


10.1. Définition

Les mouchards (spywares en anglais) sont devenus monnaie courante chez Microsoft.

Tous les systèmes d'eXPloitation Windows 98 , 98 Se, Me, 2000 et maintenant Windows XP ont tous un mouchard.

Ce mouchard est en fait un contrôle ActiveX qui permet de recueillir plusieurs informations sur vous et votre ordinateur

 votre HWID (Hardware ID), c'est à dire la configuration de votre ordinateur (matériel et/ou logiciel),

 votre MSID (Microsoft ID), code clé au verso de la boîte de Windows .

Les mouchards pour la plupart servent à faire des statistiques sur l'utilisation des logiciels et leurs utilisateurs.

Il agissent totalement à votre insu, lors d'une connexion à Internet , les informations recueillies par le mouchard sont envoyées à son créateur (pour Windows --> Microsoft).

Beaucoup de logiciels sur le marché utilisent des mouchards pour cibler les utilisateurs de leur logiciel.

Inutile de tomber dans la paranoïa !

Les informations que récoltent les mouchards sont minimes.

Toutefois si cela vous gêne d'être suivis sur Internet , voici les manipulations à effectuer pour supprimer les mouchards de Windows .

10.2. Retirer les mouchards

10.2.1. Windows XP Home :

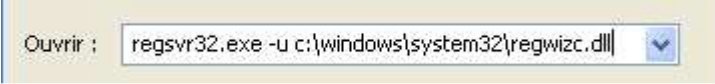
Sur le bureau de Windows , cliquez sur :

 **menu Démarrer** (cliquez ici pour tout savoir sur le menu Démarrer)

 **Exécuter** 

Dans la fenêtre qui s'ouvre, tapez :

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



Ouvrir : regsvr32.exe -u c:\windows\system32\regwizc.dll

Cliquez sur **OK**, le message suivant devrait apparaître :



Vous voilà débarrassé du mouchard de Windows XP Home.

10.2.2. Windows 2000

Suivez les même étapes que pour Windows XP Home en mettant à la place :

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

10.2.3. Windows 98/ 98 SE

Suivez les même étapes que pour Windows XP Home en mettant cette ligne de commande dans **Exécuter** :

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

10.3. récupérer votre mouchard

10.3.1. Windows XP Home

Sur le bureau, cliquez sur :

 **Démarrer**

 **Exécuter**

Tapez ensuite la ligne de commande suivante :

```
regsvr32.exe -c c:\ Windows\system\regwizc.dll puis cliquez sur OK.
```



le mouchard est réactivé.

10.3.2. Windows 2000

Procédez de la même manière que pour Windows XP Home mais avec cette ligne de commande :

```
regsvr32.exe -c c:\winnt\system32\regwizc.dll puis cliquez sur OK.
```

10.3.3. Windows 98 / 98 SE

Procédez de la même manière que pour Windows XP Home mais avec cette ligne de commande :

```
regsvr32.exe -c c:\Windows\system\regwizc.dll puis cliquez sur OK.
```

11 BLOQUER ET DÉBLOQUER LES PIÈCES JOINTES SOUS OUTLOOK EXPRESS

Depuis la version 6, Outlook EXPress permet de bloquer les e-mails susceptibles de contenir des virus.

Etape 1 : Pour activer cette protection, déroulez le menu **Outils**, puis cliquez sur **Options**. Dans l'onglet **Sécurité**, cochez la case **Ne pas autoriser l'ouverture ou l'enregistrement des pièces jointes susceptibles de contenir un virus**. Validez ensuite par **OK**. Désormais, vous ne pourrez plus ouvrir les pièces jointes avec les extensions .exe (programmes), .vbs (programmation VB Script), etc... qui sont utilisées par les virus.

Etape 2 : Décochez simplement cette même case pour rendre à nouveau accessibles les pièces jointes considérées comme dangereuses.